USER MANUAL

XRoads' EdgeXOS Platforms

XRoads Networks

UNIFIED BANDWIDTH MANAGEMENT

EdgeXOS Administrator's Guide™

Setup and Configuration

S/W VERSION 4.1

Copyright

© Copyright 2013

Vendor Trademarks

Accelibond™, Adaptiband™, ActiveDNS™, Site2Site™, XFlow Reporting™, ActiveHA™, EdgeXOS Best Path Routing™, MVP Multi-Vector Priority Routing™

Are all trademarks of XRoads Networks.

Table of Contents

Table of Contents

Copyright **i**

Vendor Trademarks **i**

Scope **16**

Audience **16**

Further Reading **16**

How to Use This Manual **18**

Product Family **18**

More Information **19**

Compliance, Safety, Quality **19**

Package Contents **22**

Pre-Installation Checklist **24**

Accessing the Appliance **24**

Physically Connecting the EdgeXOS Appliance 24

Administrative Access—WEB GUI 26

Accessing the CLI 27

CONFIGURATION: STEP ONE **29**

Pre-Installation Configuration Sheet **29**

CONFIGURATION: STEP TWO **30**

Deployment Methods **30**

Transparent Drop-In Mode Overview 31

Direct Network Address Translation (NAT) Mode Overview 31

Routing Mode Overview..... 32

CONFIGURATION: STEP THREE 33

GUI Overview 33

Login 34

Home Tab 35

Interfaces Tab 35

Interface Config Menu 36

AppShaping Tab 36

EdgeXOS Routing Menu 37

AppRouting Tab 37

NetBalancing Selection Menu 38

Site 2 Site Tab 38

XOS Tunnels List 38

Firewall Tab 39

EdgeXOS Security Menu 39

Tools Tab 40

EdgeXOS Tools Menu 40

Reporting Tab 41

Reporting Menu 41

General System Settings..... 42

Registration 42

Setting the Password 43

Setting NIC Speed/Duplex 43

Setting Email Alerts 44

Add an Email Alert 44

Setting Time/Date 46

Setting XGM Parameters 46

Link Control Configuration 47

INTERFACE CONFIGURATION 50

LAN Interface Configuration 50

WAN Interface Configuration 52

Other Interface Configurations 55

Static Routes 55

Secondary IPs 56

Secondary Bridges 57

VLAN Tagging 58

DHCP Groups 59

Application Routing Configuration 60

Active DNS Policies 67

Domain Settings 68

Host Records 69

ActiveDNS-Geo 71

Active Routing Policies 72

Outbound Application Routing—Multi-Vector Priority (MVP) Routing 73

Outbound Application Routing—Multi-Session Acceleration (MSA) 75

Outbound Application Routing—MVP Best Path Routing 78

Outbound Application Routing—MVP Application Routing 79

Add Service (MVP Application Routing) 80

Outbound Application Routing—MVP Redirect Routing 81

Add Redirect (MVP Redirect Routing) 81

In/Out Balancing Control—Vector Mappings 82

Add Service (In/Out Balancing Control Vector Mappings) 83

Inbound Application Routing—Application Proxy (VNAT) 84

Add VirtualNAT Rule (Application Proxy) 85

Inbound Application Routing—O2M NAT 87

Inbound Application Routing—O2O NAT 87

Local Server Balancing—Server Load Balancing (SLB) 88

Add SLB Group 88

Private Link Bonding 89

Application Shaping Configuration 91

Dynamic Bandwidth Management 92

DBM Session Throttling 93

Add Range (DBM Session Throttling) 94

DBM Adaptive Shaping 95

Advanced Params (DBM Adaptive Shaping) 96

Bypass Policies (DBM Adaptive Shaping) 97

Policy-Based Shaping 98

Add Policy (Policy-Based Shaping) 99

VoIP Shaping & QoS 101

Application Shaping 102

Application Mgmt 102

Create Application Rule 103

URL Shaping 104

URL Mgmt 105

Create URL Rule 106

Site2Site Configuration 107

Site2Site Overview 107

Site2Site Example Configuration 108

XOS Tunnels List 119

Add Tunnel (XOS) 119

Add Route (XOS) 124

Add Policy (XOS) 125

S2Slog 126

Firewall Overview 127

L7 Firewall Rules 128

Add Rule 129

L7 Firewall Control 131

L7 Firewall User Management 132

Add User/Device 133

L7 Firewall DoS / SYN Filtering..... 134

L7 Firewall Global Web Filtering 135

Display NAT Rules 137

Vector Routing (Outbound) 138

Add Service (Vector Routing) 138

One-To-Many NAT (PAT) 140

Add Service (One-To-Many NAT) 140

One-To-One NAT (SNAT)..... 142

Add Service (One-To-One NAT) 143

Remote Access Site2Site Client..... 145

Remote Access PPTP Client..... 148

User/Device Access Control (NAC) 148

Dashboard (Home page) Overview 150

Dashboard 150

System Commands 151

Interfaces Overview 151

Network Usage 152

Application Usage 152

URL Usage 153

Recent Activity 153

System Logs 154

File Uploads 155

XFlow Reporting Engine (XRE) 155

Link Utilization 156

Historical WAN Reporting 156

SLA Reporting 157

XFlow Bandwidth Usage 158

XFlow Graphical Reports 159

XFlow Control 160

MVP Subnet Reporting 161

Web Filter URL Reporting 162

Web Filter Live Reporting 162

Web Filter Usage Reporting 163

Device Monitoring 163

Firewall Logs 164

System Logs 164

Registration 166
SNMP/XGM Control 166
Virtual Technician 167
Time/Date Setting 168
Remote Access 168
Admin Access 169
Email Alerts 169
Ping 169
Port Speed / Duplex 169
Route Table 169
Arp Table 170
Hardware High Availability 170
Primary Unit Configuration 175
Secondary Unit Configuration 177
Post Failover Procedures..... 178

Copyright i
Vendor Trademarks i
Table of Contents ii
Scope 16
Audience 16
Further Reading 16
Introduction to EdgeXOS with Unified Bandwidth Management™ 17
How to Use This Manual..... 18
Product Family 18

More Information 19

Compliance, Safety, Quality 19

License 20

GETTING STARTED - EdgeXOS Overview 22

Package Contents 22

Pre-Installation Checklist 24

Accessing the Appliance 24

Physically Connecting the EdgeXOS Appliance 24

Administrative Access—WEB GUI 26

Accessing the CLI 27

CONFIGURATION: STEP ONE 29

Pre-Installation Configuration Sheet 29

CONFIGURATION: STEP TWO 30

Deployment Methods 30

Transparent Drop-In Mode Overview 31

Direct Network Address Translation (NAT) Mode Overview 31

Routing Mode Overview 32

CONFIGURATION: STEP THREE 33

GUI Overview 33

Login 34

Home Tab 35

Interfaces Tab 35

Interface Config Menu 36

AppShaping Tab 36

EdgeXOS Routing Menu 37

AppRouting Tab 37

NetBalancing Selection Menu 38

Site 2 Site Tab 38

XOS Tunnels List 38

Firewall Tab 39

EdgeXOS Security Menu 39

Tools Tab 40

EdgeXOS Tools Menu 40

Reporting Tab 41

Reporting Menu 41

UBM Initial Installation and Configuration Steps 42

General System Settings 42

Registration 42

Setting the Password 43

Setting NIC Speed/Duplex 43

Setting Email Alerts 44

Add an Email Alert..... 44

Setting Time/Date 46

Setting XGM Parameters 46

Link Control Configuration 47

INTERFACE CONFIGURATION 50

LAN Interface Configuration..... 50

WAN Interface Configuration 52

Other Interface Configurations 55

Static Routes 55

Secondary IPs 56

Secondary Bridges 57

VLAN Tagging 58

DHCP Groups 59

Application Routing Configuration 60

Active DNS Policies 67

Domain Settings 68

Host Records 69

ActiveDNS-Geo 71

Active Routing Policies 72

Outbound Application Routing—Multi-Vector Priority (MVP) Routing 73

Outbound Application Routing—Multi-Session Acceleration (MSA) 75

Outbound Application Routing—MVP Best Path Routing 78

Outbound Application Routing—MVP Application Routing 79

Add Service (MVP Application Routing) 80

Outbound Application Routing—MVP Redirect Routing 81

Add Redirect (MVP Redirect Routing) 81

In/Out Balancing Control—Vector Mappings 82

Add Service (In/Out Balancing Control Vector Mappings) 83

Inbound Application Routing—Application Proxy (VNAT) 84

Add VirtualNAT Rule (Application Proxy) 85

Inbound Application Routing—O2M NAT 87

Inbound Application Routing—O2O NAT 87

Local Server Balancing—Server Load Balancing (SLB) 88

Add SLB Group 88

Private Link Bonding 89

Application Shaping Configuration 91

Dynamic Bandwidth Management 92

DBM Session Throttling 93

Add Range (DBM Session Throttling) 94

DBM Adaptive Shaping 95

Advanced Params (DBM Adaptive Shaping) 96

Bypass Policies (DBM Adaptive Shaping) 97

Policy-Based Shaping 98

Add Policy (Policy-Based Shaping) 99

VoIP Shaping & QoS 101

Application Shaping 102

Application Mgmt 102

Create Application Rule 103

URL Shaping 104

URL Mgmt 105

Create URL Rule 106

Site2Site Configuration 107

Site2Site Overview 107

Site2Site Example Configuration 108

XOS Tunnels List 119

Add Tunnel (XOS) 119

Add Route (XOS) 124

Add Policy (XOS) 125

S2Slog 126

Security and Firewall Features 127

Firewall Overview 127

L7 Firewall Rules 128

Add Rule 129

L7 Firewall Control 131

L7 Firewall User Management 132

Add User/Device 133

L7 Firewall DoS / SYN Filtering 134

L7 Firewall Global Web Filtering 135

Display NAT Rules 137

Vector Routing (Outbound) 138

Add Service (Vector Routing) 138

One-To-Many NAT (PAT) 140

Add Service (One-To-Many NAT) 140

One-To-One NAT (SNAT) 142

Add Service (One-To-One NAT) 143

Remote Access Site2Site Client 145

Remote Access PPTP Client 148

User/Device Access Control (NAC) 148

Monitoring and Reporting Capabilities 150

Dashboard (Home page) Overview..... 150

Dashboard 150

System Commands 151

Interfaces Overview 151

Network Usage 152

Application Usage 152

URL Usage 153

Recent Activity 153

System Logs 154

File Uploads 155

XFlow Reporting Engine (XRE)..... 155

Link Utilization 156

Historical WAN Reporting 156

SLA Reporting 157

XFlow Bandwidth Usage 158

XFlow Graphical Reports 159

XFlow Control 160

MVP Subnet Reporting 161

Web Filter URL Reporting 162

Web Filter Live Reporting 162

Web Filter Usage Reporting 163

Device Monitoring 163

Firewall Logs 164

System Logs 164

Tools **166**

Registration 166

SNMP/XGM Control 166

Virtual Technician 167

Time/Date Setting 168

Remote Access 168

Admin Access *169*

Email Alerts *169*

Ping *169*

Port Speed / Duplex *169*

Route Table *169*

Arp Table *170*

Hardware High Availability *170*

Appendix A - Factory Default 171

Appendix B – Troubleshooting 173

Appendix C - Hardware High Availability (HA) Configuration 174

Primary Unit Configuration 175

Secondary Unit Configuration 177

Post Failover Procedures 178

Appendix D - CLI Menu Overview 179

Appendix E - Glossary and Definitions 182

Appendix F - How To Get Assistance 185

Scope

The scope of this document is designed to cover the basic installation and overview of the EdgeXOS platforms web GUI and basic functionality. For more details on any specific functionality and/or the configuration of said functionality, please reference our How To Guides, available via the XRoads Networks website under the Support section.

Audience

This document is intended for network engineers and/or IT administrators who have a background in networking and understand basic subnetting and IP infrastructure.

Further Reading

- XRoads Networks recommends reading over the various support materials available on our website via the Support / Documentation link.
- Please use our support site www.myxroads.com to access frequently asked questions and to get additional assistance through our support system. The fastest way to obtain technical support is to open a new support ticket via the MYXROADS.com website.

Introduction to EdgeXOS with Unified Bandwidth Management™

EdgeXOS…

Unified Bandwidth Management (UBM) is designed to improve responsiveness and reliability of Internet and cloud-based applications through a combination of network management technologies. These technologies are delivered via either a SingleSite or a Site2Site solution and include the following capabilities:

Application Shaping & QoS: The ability to accelerate and filter web traffic and prioritize mission critical applications while reporting on network usage.

Application Routing & Balancing: The ability to combine multiple Internet connections to obtain faster network speeds and improved redundancy in the event of an ISP outage.

Application WAN Optimization & Redundancy: Our Site2Site feature set provides the ability to connect multiple offices and optimize those connections for better performance and faster downloads between sites.

How to Use This Manual

This user manual provides detailed instructions on how to use the EdgeXOS platform. Specific instructions are given for the configuration and use of the device, please reference the table of contents to find your specific area of interest.

Throughout the manual the following text styles are used to highlight important points:

- Useful features, hints and important issues are called "notes" and they are identified in a **blue background**.

NOTE	Notes provide tips and background information for the task at hand.

- Examples are identified in a **green background**.

EXAMPLE	Examples provide sample settings for the task at hand.

- Warnings are identified in a **yellow background**.

CAUTION	Cautions provide warnings for the task at hand.

-

Product Family

- This document covers the entire EdgeXOS hardware product family, including both the aXcel and UBM series of products. The differences between the series are primarily licensing and hardware variants,

the interface and configuration of available features are the same between solutions.

More Information

- Please contact XRoads Networks at 888-997-6237.

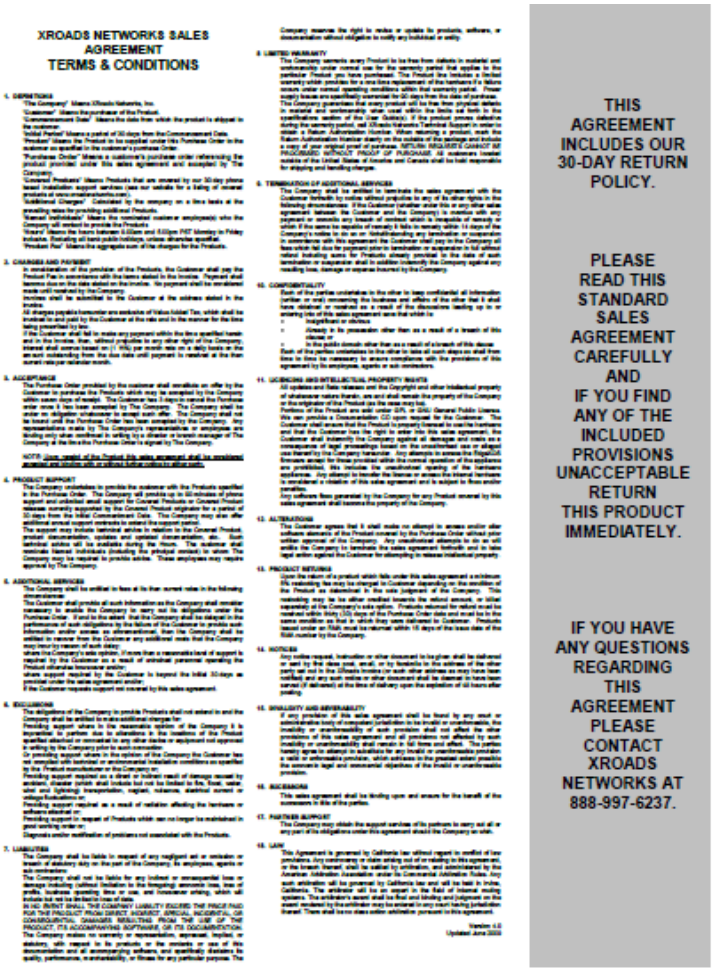
Compliance, Safety, Quality

All XRoads Networks products are UL rated and meet US Federal Communications Commission requirements and specifications.

XRoads Networks hardware products also meet RoHS requirements for easy disposal and have been certified by various international regulatory bodies. Please contact XRoads Networks for further details on specific certifications.

License

A license has been included in the packaging for your EdgeXOS platform, please reference it for the latest version and/or visit our website for full licensing information. The license included within the packaging should look something like this:



XROADS NETWORKS SALES AGREEMENT
TERMS & CONDITIONS

THIS AGREEMENT INCLUDES OUR 30-DAY RETURN POLICY.

PLEASE READ THIS STANDARD SALES AGREEMENT CAREFULLY AND IF YOU FIND ANY OF THE INCLUDED PROVISIONS UNACCEPTABLE RETURN THIS PRODUCT IMMEDIATELY.

IF YOU HAVE ANY QUESTIONS REGARDING THIS AGREEMENT PLEASE CONTACT XROADS NETWORKS AT 888-997-6237.

If you have any questions about the EdgeXOS platform license please contact XRoads Networks at 888-997-6237 or email us at corporate@xroadsnetworks.com. Thank you.

GETTING STARTED - EdgeXOS Overview

The EdgeXOS platform is a Unified Bandwidth Management device, meaning that it has the ability to support multiple bandwidth management functions, including: Next generation WAN Link Bonding & Balancing, Automated Network Failover, Web Acceleration, Traffic Shaping & QoS, Network Monitoring & Reporting, and Site2Site Link Bonding w/Built-In Redundancy.

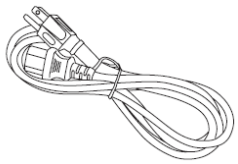
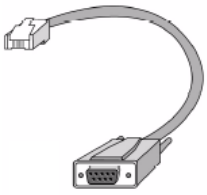
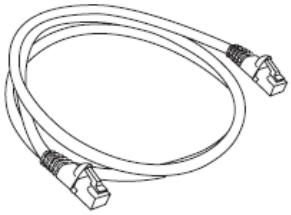
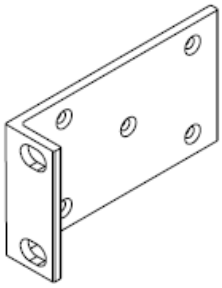
Beyond these various capabilities, the EdgeXOS platform is also highly flexible when it comes to setup and installation. This guide is designed to assist new customers with planning their installation so that it meets their unique requirements. Use the examples provided below to determine which installation method is best for your environment based on your specific requirements.

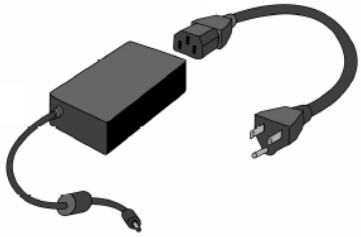
We hope that you enjoy the capabilities that the EdgeXOS platform provides, thank you for your purchase of our products, and please provide us with feedback by going to the XRoads Networks website and filling out our online survey.

Package Contents

Within the packaging of your EdgeXOS appliance you will find a number of cables, including an AC power cable. In some versions of the EdgeXOS platform you may also find a console cable and/or a CAT5 Ethernet cable and rack mount brackets (again this depends on the model). Some models also include an external power supply which has full range support for international installations.

- AC Power Cable

- 
- Console Cable
- 
- CAT5 Ethernet Cable
- 
- Rack Mount Kit
- 
- External Power Supply



Pre-Installation Checklist

Before powering up the appliance make sure that the appliance is not connected to the rest of your network. This could cause IP address conflicts if another device on your network is using the same address.

NOTE	By default the appliance boots with an IP address of 192.168.168.254 Subnet Mask 255.255.255.0

Connect your laptop/desktop directly to the EdgeXOS appliance via a Ethernet cable. Use the LAN port of the EdgeXOS appliance when connecting. Make sure that the computer you intend to use for configuring has an IP address assigned to the NIC within the 192.168.168.x range and has a subnet of 255.255.255.0.

Accessing the Appliance

In order to access and configure the appliance, the first step is to connect to the appliance via an Ethernet cable, the following outlines that process.

Physically Connecting the EdgeXOS Appliance

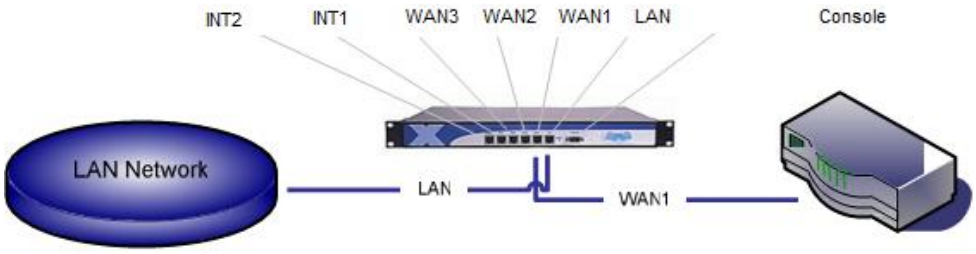
By default the EdgeXOS appliance is configurable from either the LAN Ethernet interface or the console port. In order to access the web-based GUI, you must

first connect a PC running a web browser to the appliance via an IP network connection.

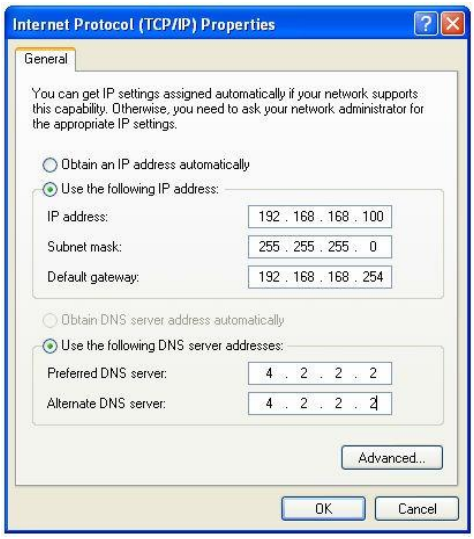
The EdgeXOS uses standard Ethernet ports (either 10/100 or 10/100/1000 depending on the model) and can be connected directly to a PC via a standard crossover cable, or to any standard Ethernet switch or hub.

Use the link lights on the Ethernet interface to verify that you have Layer 1 connectivity. When properly connected the interface should show a green light. A flashing yellow or orange light may also appear, this designates that traffic is coming in or going out of the interface.

Interfaces Overview: Use the LAN (local area network) interface to connect the internal network. Use the WAN (wide-area network) interfaces to connect to the external networks or Internet. The INT interfaces can be used as either WAN or DMZ interfaces. When used as DMZ interfaces they do not perform connectivity testing or participate in load balancing, they are simply routed ports. Use the console port for local CLI access.

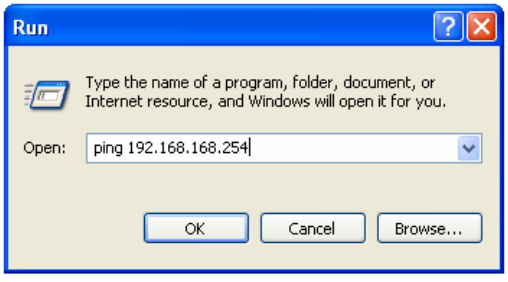


Once you have a green light on the LAN interface, change your computers network settings so that it will reside on the same network as the EdgeXOS appliance, see example:


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 168 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 168 . 254
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 4 . 2 . 2 . 2
Alternate DNS server: 4 . 2 . 2 . 2
Advanced...
OK
Cancel

Administrative Access—WEB GUI

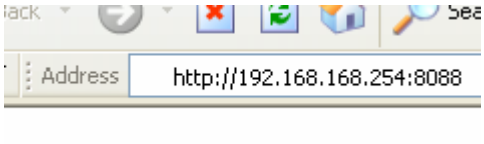
When connecting to the EdgeXOS appliance you should first perform a PING operation to make sure that your computer is able to access the appliance over the network. This operation can be conducted on a Windows system via the Start menu. The image below shows how to run this test:


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open: ping 192.168.168.254
OK
Cancel
Browse...

You should get back a reply response from the ping test. If you do not, then your computer is not setup on the correct network, or the appliance is not properly connected to the network.

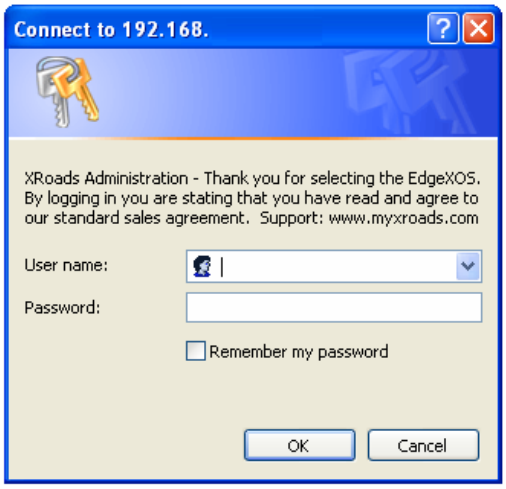
Once you are able to ping the appliance the next step is to open a web browser and enter the URL http://192.168.168.254:8088. This is the default IP address of

the LAN interface for the EdgeXOS appliance. The 8088 is the default administrator web port.



You must include the http:// portion any time you use a direct IP address in your URL or the connection will not work.

Next you will be prompted for a login and password. The default login username is **admin**, the default login password is **password**. Enter these in the popup window in order to log in to the appliance. This will grant you access to the Home page of the device


Connect to 192.168.
XRoads Administration - Thank you for selecting the EdgeXOS. By logging in you are stating that you have read and agree to our standard sales agreement. Support: www.myxroads.com
User name:
Password:
Remember my password
OK
Cancel

Accessing the CLI

The CLI or command line interface is actually a menu driven system which is accessible via either SSH or through a console port connection and provides access to many common troubleshooting tools like ping and traceroute, the ability to view route and interface information, the ability to add secondary

interface IP addresses, and the ability to modify the text configuration file via the command line.

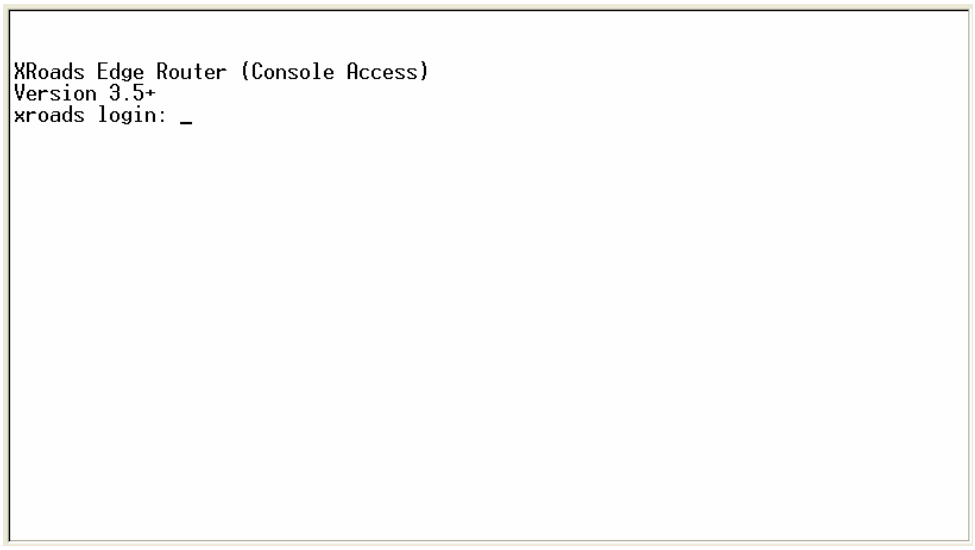
SSH access can be made by connecting to port 2022 via the LAN interface. Access is also available via the WAN interfaces when remote access is enabled. This must be initially configured via the web GUI.

Console access can be obtained via the console port:

Newer console ports use an interface that looks like an Ethernet interface, but it will be correctly labeled as a CONSOLE port. Be sure not to confuse the two.

By using a terminal application (like HyperTerminal in Windows) you can connect to the console port via a console cable (one is provided with the appliance packaging). The standard settings for the console connection are 9600bps, Data bits 8, Parity none, Stop bits 1, Flow Control Hardware. Our latest EdgeXOS firmware uses 19200bps instead of 9600bps for the connection speed.

Note: Flow Control must be set to 'none' for the smaller Edge2WAN models.



Once connected a login prompt will appear, simply enter the current login and password information as you would use for the web GUI. The default login is 'admin', the default password is 'password'.

CONFIGURATION: STEP ONE

Pre-Installation Configuration Sheet

The first step of any EdgeXOS appliance should be the filling out of the Installation Configuration Sheet. This sheet would have been provided to you by your XRoads Networks sales representative and/or installation coordinator.

The three most important aspects of this sheet include:

1. Identifying the deployment method, i.e. Route, NAT, Bridge mode.

2. Details on this step can be found below, but the general guidelines are, NAT mode is the default method, Bridge mode is used if you have an existing subnet passed to an

internal firewall, and Route mode is used for more complicated deployments, and/or deployments which involve VLANs.

3. Determining the proper IP addressing.

4. Each WAN interface address and gateway.

5. The LAN interface address and subnet information.

6. Traceroute response to determine the best probe address.

7. Outlining the tests which you will perform to make sure that everything is setup correctly for your specific environment.

8. This includes any specific application testing, email, mission critical web site access, and any other commonly used application testing.

9. Failover testing (if multiple WAN links are deployed), including testing inbound access for internal servers.

10.

CONFIGURATION: STEP TWO

Deployment Methods

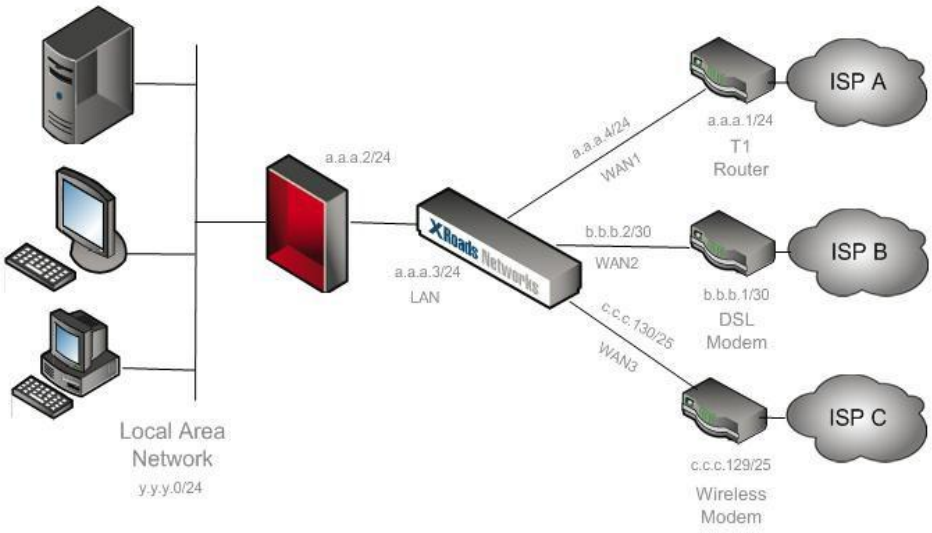
This step can be completed as part of step one, but must be completed prior to step three. Determining the deployment method is important as it determines how your EdgeXOS appliance will function and what capabilities it will have within your network.

Outlined below are the various methods for deployment, please read over each and use the guidelines to determine the best method for your network.

Transparent Drop-In Mode Overview

The “transparent drop-in mode” or bridge mode allows the EdgeXOS appliance to sit between an existing gateway router and LAN network without changing the existing IP addressing within that network.

This means that the installation of the appliance is truly “transparent”. The key to this type of installation is making sure that the device is placed directly between the gateway router and the rest of the LAN-facing network. Only the gateway address of the router can be seen on the WAN1 interface, no other addresses will be permitted to exist on the WAN1 interface and still be seen by the LAN side of the EdgeXOS device (see the diagram below for an example).

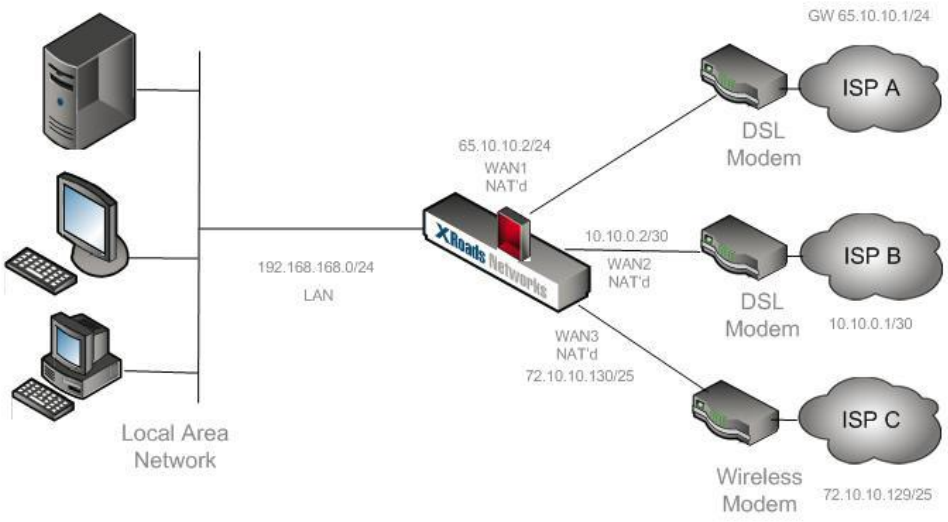


Direct Network Address Translation (NAT) Mode Overview

This mode is designed to be used when you have only a small number of public addresses, or when the EdgeXOS appliance will take over for an existing firewall.

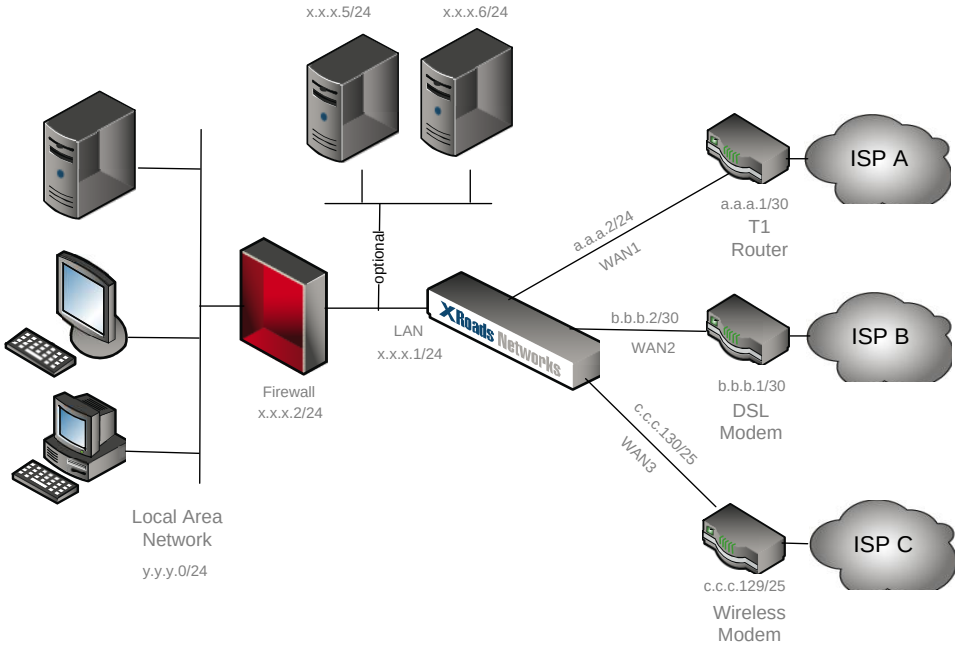
This method may require some changes to your existing network; however when configured in this mode all of the features and capabilities of the appliance can be fully enabled.

NOTE: If possible this is the recommended method for pre-firewall configurations.



Routing Mode Overview

This method provides the most functionality and is generally the easiest to configure; however it may require changes to your existing network architecture, including placing a subnet between the firewall and the EdgeXOS appliance.



CONFIGURATION: STEP THREE

GUI Overview

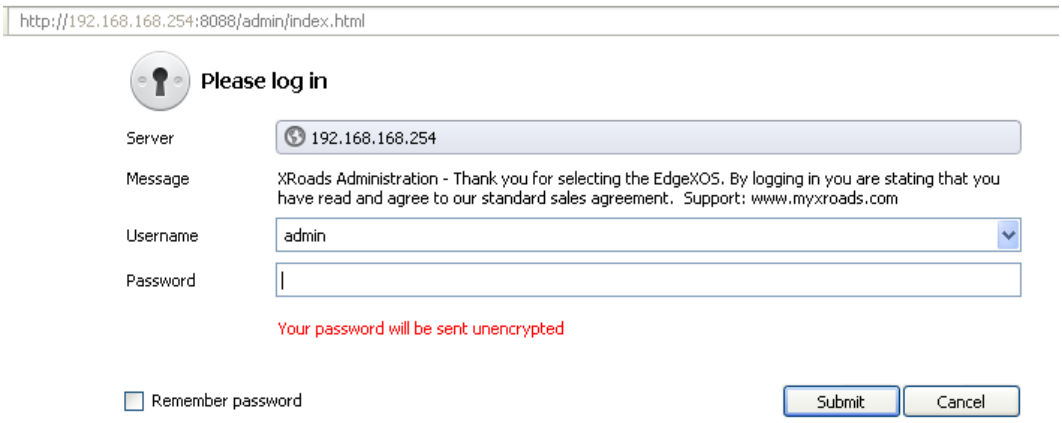
You access the EdgeXOS administrator's interface via a browser pointed to the IP address of the LAN interface, by default this is 192.168.168.254. Always use port 8088 from the LAN side to access the appliance. When accessing from the WAN you can use either 8088 or 44380 (secure SSL access).

The URL should look like the following – http://192.168.168.254:8088

Make sure to include the 'http://' at the beginning and the ':8088' at the end. Some browsers will not work correctly without the full URL being entered as shown.

Login

An authentication dialog box requires credentials:

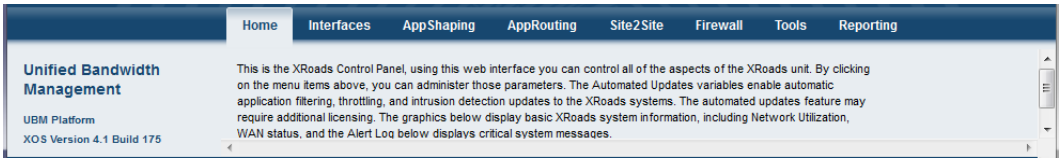


Open one of the tabs at the top to access other pages, including:

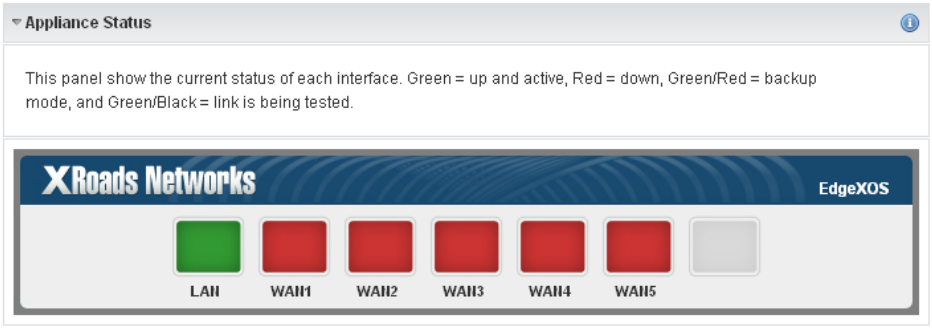
- Home Tab
- Interfaces Tab
- AppShaping Tab
- AppRouting Tab
- Site 2 Site Tab
- Firewall Tab
- Tools Tab
- Reporting Tab

Home Tab

The opening page, **Home**, provides a dashboard and several graphs of your configuration. Open an area of the **Home** page to see relevant commands or information. Find the EdgeXOS appliance version in the left pane. For a description of each graph, see the Monitoring and Reporting capabilities section and specifically the Dashboard section therein.


Home
Interfaces
AppShaping
AppRouting
Site2Site
Firewall
Tools
Reporting
Unified Bandwidth Management
UBM Platform
XOS Version 4.1 Build 175
This is the XRoads Control Panel, using this web interface you can control all of the aspects of the XRoads unit. By clicking on the menu items above, you can administer those parameters. The Automated Updates variables enable automatic application filtering, throttling, and intrusion detection updates to the XRoads systems. The automated updates feature may require additional licensing. The graphics below display basic XRoads system information, including Network Utilization, WAN status, and the Alert Log below displays critical system messages.

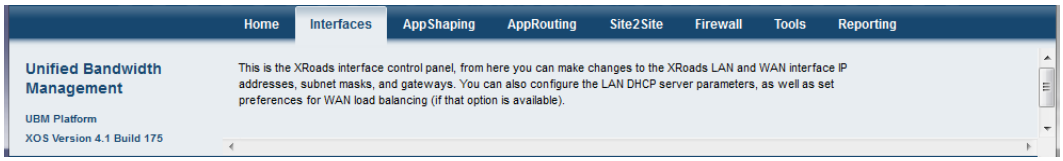
The first section of the Home page Dashboard demonstrates the status of the various links, this is critical to determining whether the EdgeXOS platform is connected to the Internet and/or if there is a problem with the WAN links. If the WAN link is RED, it is down, if GREEN it is up, and if GREEN but with a TESTING notice, it means that it is attempting the bring up the interface but has yet to confirm its availability.



Interfaces Tab

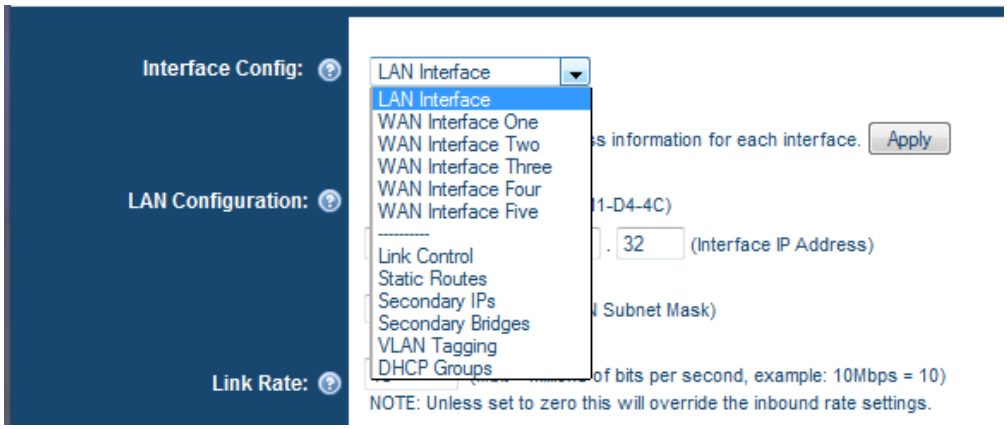
This is the **Interface** control panel, from here you can make changes to the XRoads LAN and WAN interface IP addresses, subnet masks, and gateways.

You can also configure the LAN DHCP server parameters, as well as set preferences for WAN load balancing (if that option is available).


Home
Interfaces
AppShaping
AppRouting
Site2Site
Firewall
Tools
Reporting
Unified Bandwidth Management
UBM Platform
XOS Version 4.1 Build 175
This is the XRoads interface control panel, from here you can make changes to the XRoads LAN and WAN interface IP addresses, subnet masks, and gateways. You can also configure the LAN DHCP server parameters, as well as set preferences for WAN load balancing (if that option is available).

Interface Config Menu

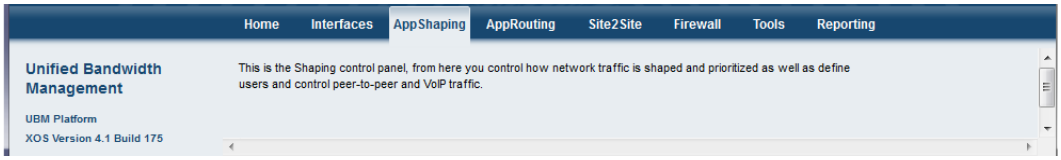
The **Interface Config** options fall into eleven groups as shown below.



AppShaping Tab

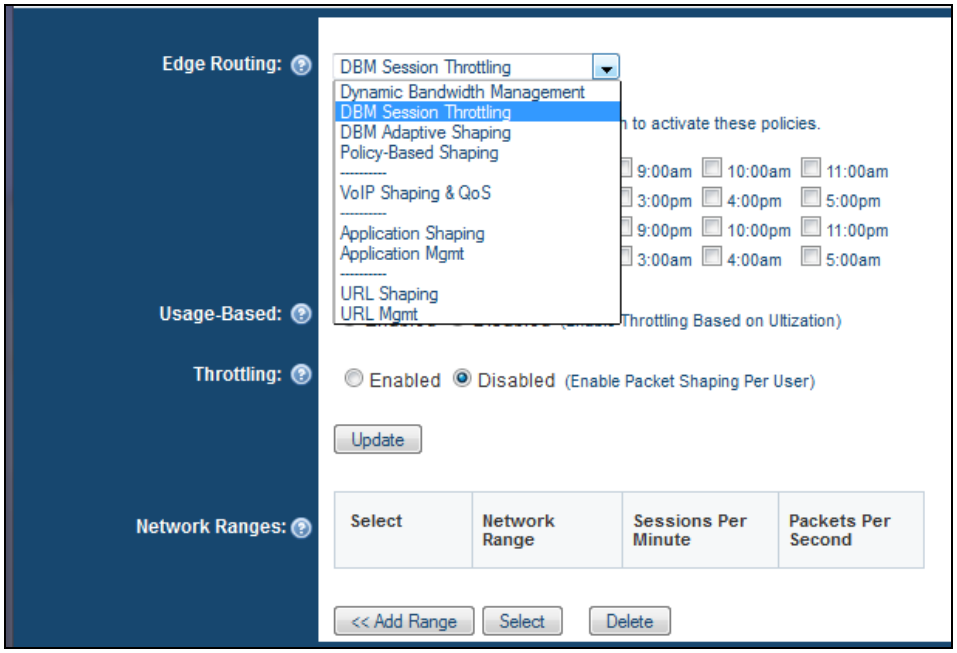
This is the **AppShaping** control panel, from here you control how network traffic is shaped and prioritized as well as define users and control peer-to-peer and VoIP traffic.

The **AppShaping** module enables the control and prioritization of network traffic as it traverses the EdgeXOS appliance. An administrator can choose to either define individual users or simply apply general application shaping rules. Enabling application shaping is the easiest way to get started. Scope-based and Policy-based rules provide more granular bandwidth control.



EdgeXOS Routing Menu

The **EdgeXOS Routing** options fall into nine groups as shown below.



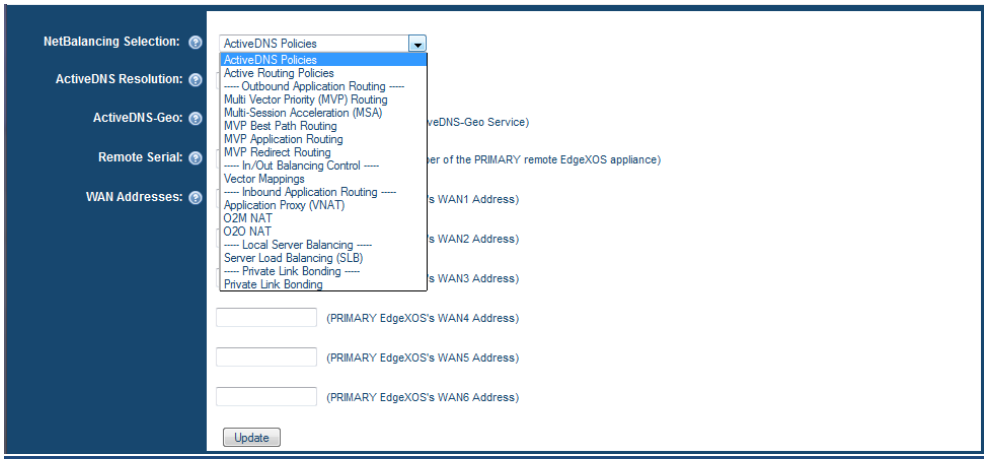
AppRouting Tab

This is the **AppRouting** control panel for NetBalancing, where you control how inbound network address translation is enabled on any of your WAN interfaces. Example: If you are using 192.168.168.0/24 space for your LAN and your web server is located at 192.168.168.10, then you would create a services rule to pass all inbound web services via web port 80 to 192.168.168.10. Make sure to **Save** any changes made in this section or they will be lost upon reboot.

Home
Interfaces
AppShaping
AppRouting
Site2Site
Firewall
Tools
Reporting
Unified Bandwidth Management
UBM Platform
XOS Version 4.1 Build 175
This is the NetBalancing control panel, from here you can control how inbound network address translation is enabled on any of your WAN interfaces. Example: If you are using 192.168.168.0/24 space for your LAN and your web server is located at 192.168.168.10, then you would create a services rule to pass all inbound web services via web port 80 to 192.168.168.10. Make sure to Save any changes made in this section or they will be lost upon reboot.

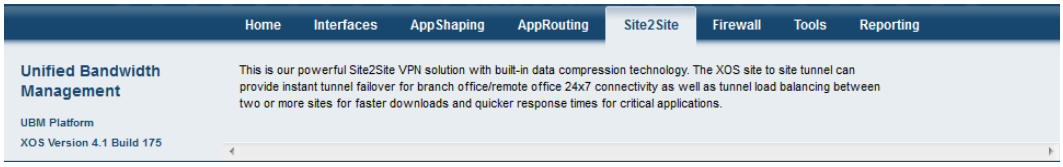
NetBalancing Selection Menu

The **NetBalancing Selection** options fall into seven groups. Each group's settings are described in the following sections.



Site 2 Site Tab

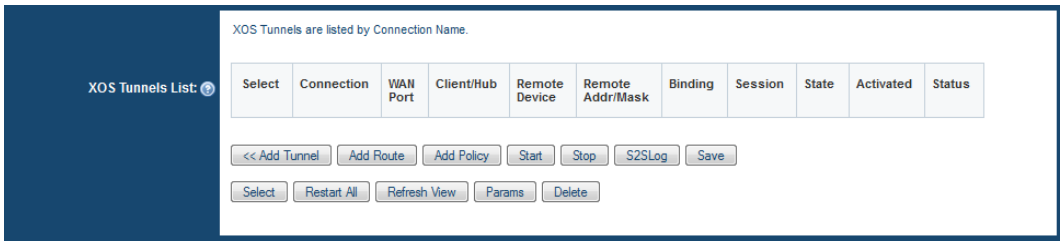
This is the **Site2Site** VPN solution with built-in data compression technology. The XOS site to site tunnel can provide instant tunnel failover for branch office/remote office 24x7 connectivity as well as tunnel load balancing between two or more sites for faster downloads and quicker response times for critical applications.


Home
Interfaces
AppShaping
AppRouting
Site2Site
Firewall
Tools
Reporting
Unified Bandwidth Management
UBM Platform
XOS Version 4.1 Build 175
This is our powerful Site2Site VPN solution with built-in data compression technology. The XOS site to site tunnel can provide instant tunnel failover for branch office/remote office 24x7 connectivity as well as tunnel load balancing between two or more sites for faster downloads and quicker response times for critical applications.

XOS Tunnels List

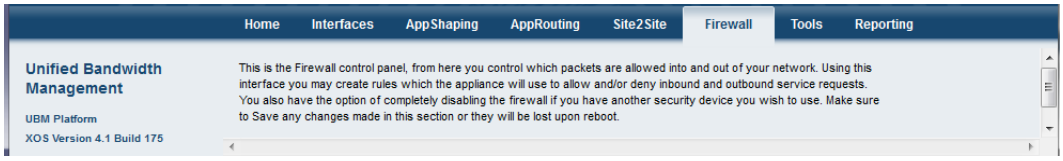
This is a listing of all currently configured WAN Optimization tunnels.

For detailed information on adding an XOS Tunnel, see our Site2Site How To Guides.



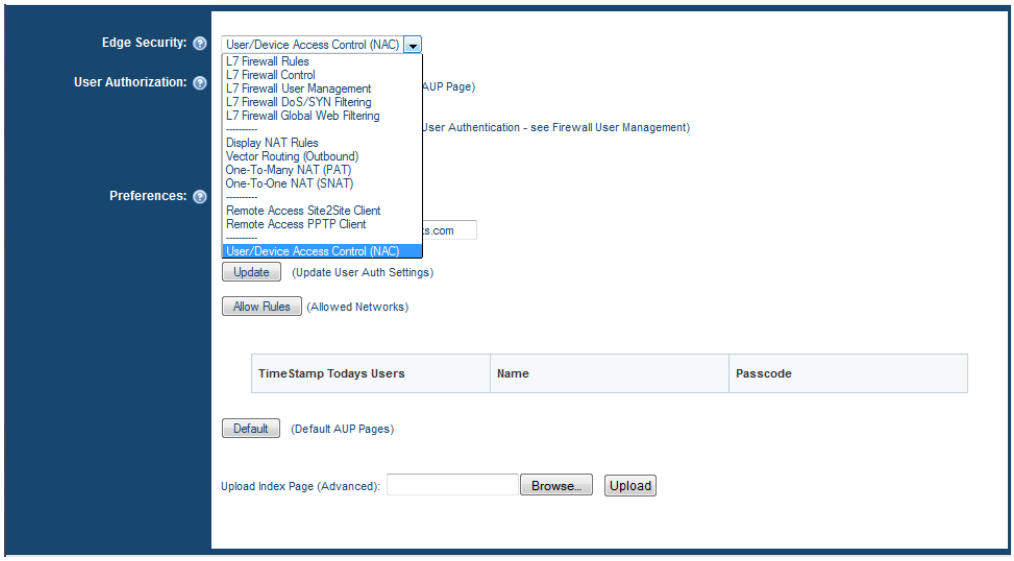
Firewall Tab

This is the **Firewall** control panel, from here you control which packets are allowed into and out of your network. Using this interface you may create rules which the appliance will use to allow and/or deny inbound and outbound service requests. You also have the option of completely disabling the firewall if you have another security device you wish to use. Make sure to Save any changes made in this section or they will be lost upon reboot.


Home
Interfaces
AppShaping
AppRouting
Site2Site
Firewall
Tools
Reporting
Unified Bandwidth Management
UBM Platform
XOS Version 4.1 Build 175
This is the Firewall control panel, from here you control which packets are allowed into and out of your network. Using this interface you may create rules which the appliance will use to allow and/or deny inbound and outbound service requests. You also have the option of completely disabling the firewall if you have another security device you wish to use. Make sure to Save any changes made in this section or they will be lost upon reboot.

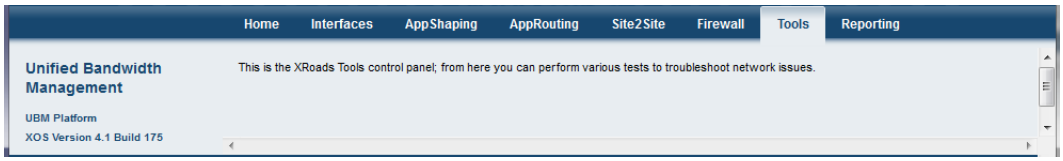
EdgeXOS Security Menu

Use this drop-down to select the security attributes you wish to administer.
NOTE: Some features may require additional licensing.

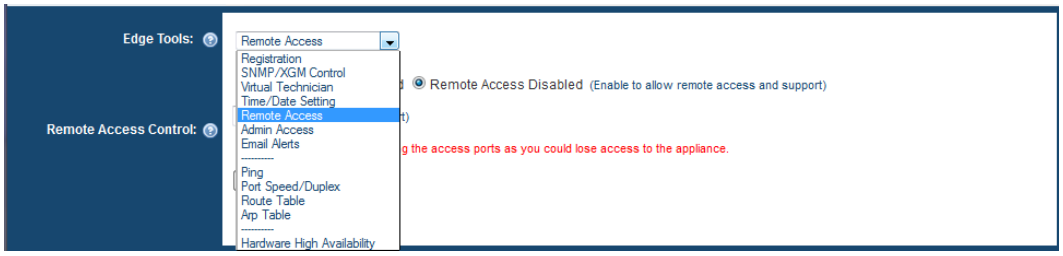


Tools Tab

This is the XRoads **Tools** control panel; from here you can perform various tests to troubleshoot network issues.

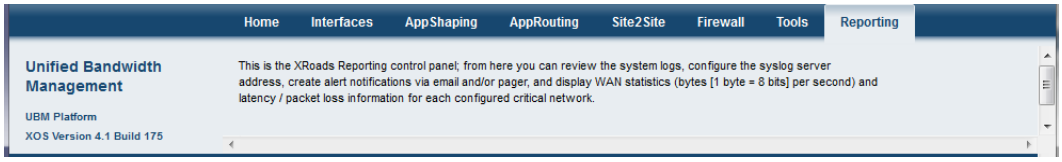


EdgeXOS Tools Menu



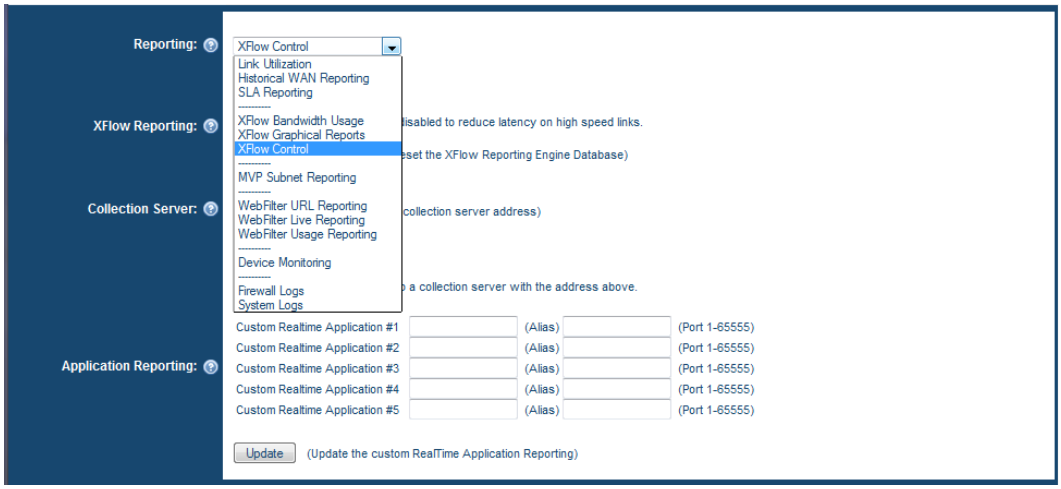
Reporting Tab

This is the XRoads **Reporting** control panel; from here you can review the system logs, configure the syslog server address, create alert notifications via email and/or pager, and display WAN statistics (bytes [1 byte = 8 bits] per second) and latency / packet loss information for each configured critical network.


Home
Interfaces
AppShaping
AppRouting
Site2Site
Firewall
Tools
Reporting
Unified Bandwidth Management
UBM Platform
XOS Version 4.1 Build 175
This is the XRoads Reporting control panel; from here you can review the system logs, configure the syslog server address, create alert notifications via email and/or pager, and display WAN statistics (bytes [1 byte = 8 bits] per second) and latency / packet loss information for each configured critical network.

Reporting Menu

The reporting menu allows you to view network graphs on each of the WAN interfaces as well as defined critical networks, add/edit alert emails, and setup a syslog server where outages and other system notifications can be directed.



UBM Initial Installation and Configuration Steps

Upon initial access to the EdgeXOS platform via the web GUI, it is important to complete the following initial configuration steps as outlined below.

General System Settings

Access the following sections within the appliance in order to complete these initial steps:

Registration

Setting the Password

Setting NIC Speed/Duplex

Setting Email Alerts

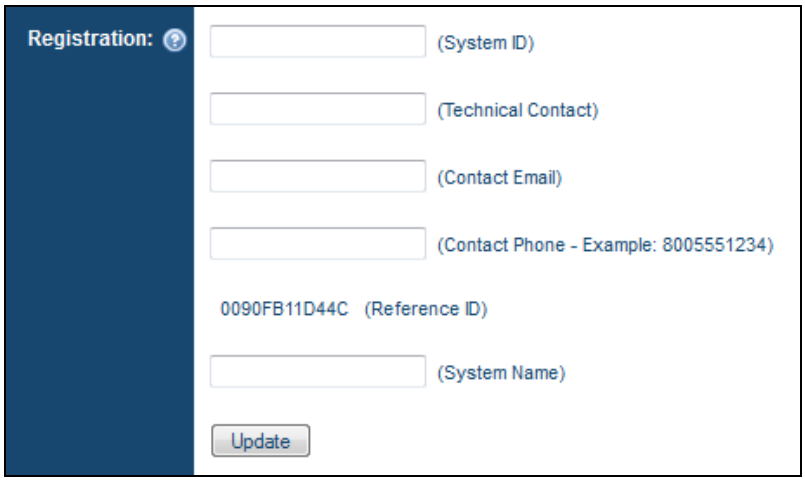
Setting Time/Date

Setting XGM Parameters

Link Control Configuration

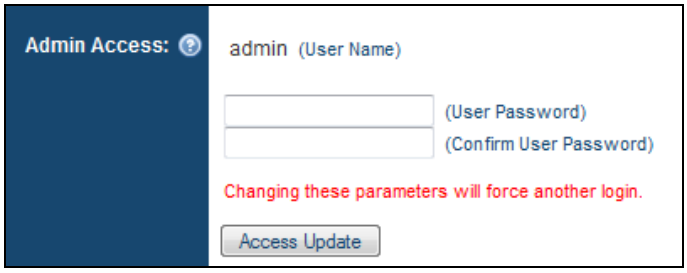
Registration

Choose **Registration** in the **Tools** tab **EdgeXOS Tools** menu and fill the form to register your XRoads unit with technical support. None of this information will ever be released; it will only be used to assist in the support this unit.



Setting the Password

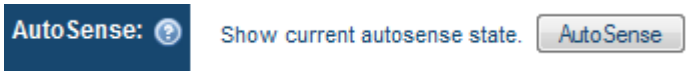
Choose **Admin Access** in the **Tools** tab **EdgeXOS Tools** menu to update your administrative passwords. NOTE: This controls all access to the XRoads unit, be sure to write down any changes to ensure you don't lose access to this unit.



Setting NIC Speed/Duplex

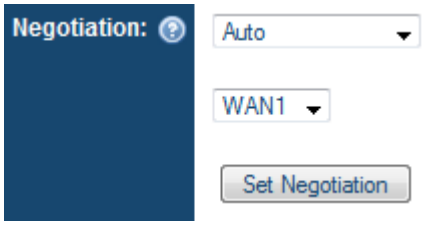
TBW

Tools > EdgeXOS Tools > Port Speed / Duplex



Use this to identify what speed and duplex the links connected to the XRoads are set at.

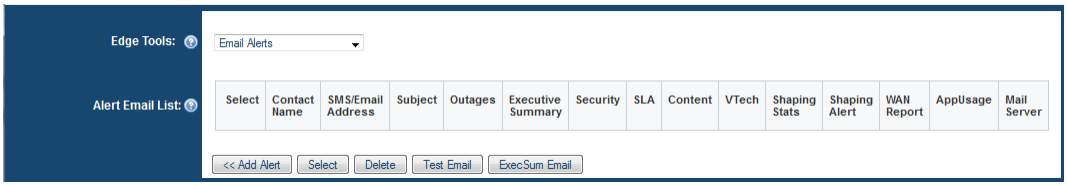
Tools > EdgeXOS Tools > Port Speed / Duplex



Use this to set the Ethernet negotiation rate for the selected link. The default negotiation is AUTO.

Setting Email Alerts

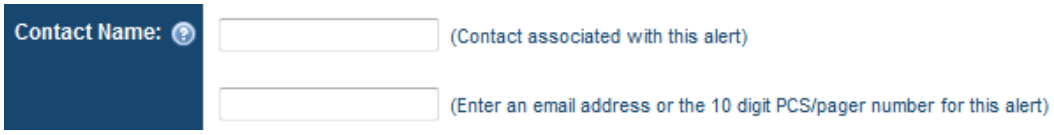
Choose **Email Alerts** in the **Tools** tab **EdgeXOS Tools** menu to a listing of all alert emails that have been configured. When an alert occurs, the associated email addressee will be notified.



Add an Email Alert

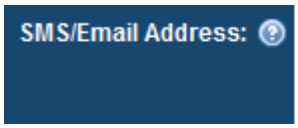
TBW

Tools > EdgeXOS Tools > Email Alerts > Add Email Alert

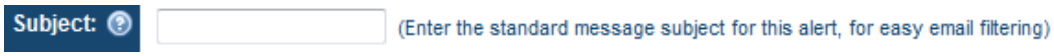


Enter the name of the person who will receive these messages.

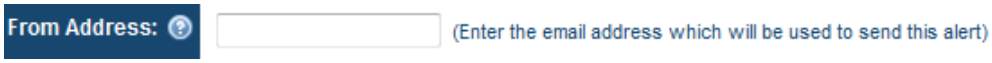
Tools > EdgeXOS Tools > Email Alerts > Add Email Alert



This is a listing of all alert emails that have been configured. When an alert occurs, the associated Enter the email address of the mailbox to receive these alerts. Example: support@abc.com



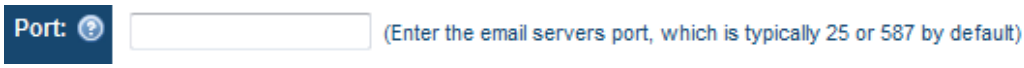
Enter a subject which can be used for email filtering. Example: XRoads Alerts



Enter the email address which will be specified in the FROM field of the email message. Example: no-reply@abc.com

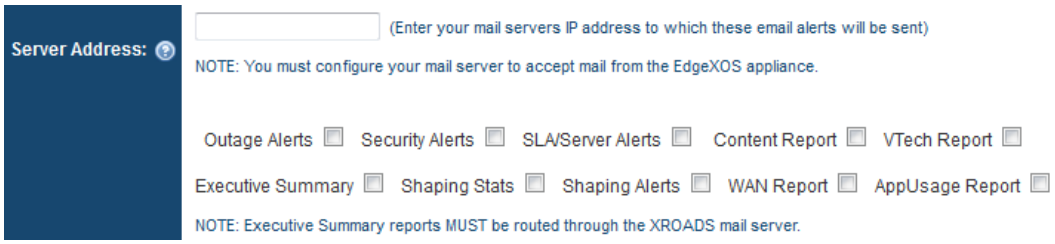
Enter the login name used to access this SMTP email account. Example: jsmith
Note that this is not typically the full email address.

Enter the login password used to access this SMTP email account.



Enter the TCP port which is used to access this SMTP server, typically either port 25 or 587.

Tools > EdgeXOS Tools > Email Alerts > Add Email Alert

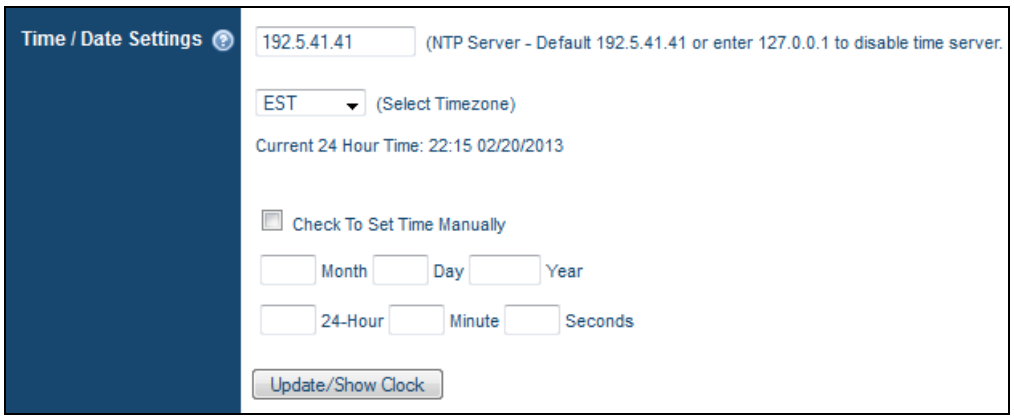

Server Address:
(Enter your mail servers IP address to which these email alerts will be sent)
NOTE: You must configure your mail server to accept mail from the EdgeXOS appliance.
Outage Alerts
Security Alerts
SLA/Server Alerts
Content Report
VTech Report
Executive Summary
Shaping Stats
Shaping Alerts
WAN Report
AppUsage Report
NOTE: Executive Summary reports MUST be routed through the XROADS mail server.

Enter the IP address of the mail server which the XRoads router will use when sending out email.

Example: 1.1.1.1

Setting Time/Date

Choose **Time/Date Setting** in the **Tools** tab **EdgeXOS Tools** menu to change the XRoads system clock which is used for logging and reporting timestamps.

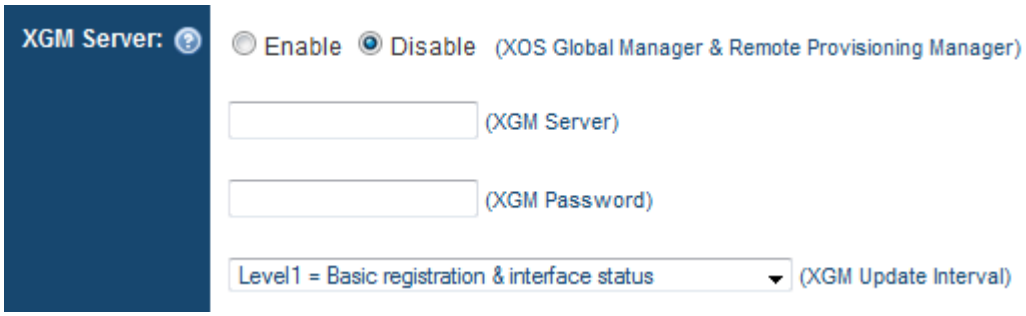


Setting XGM Parameters

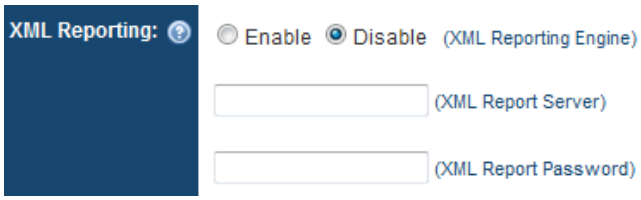
Click **XGM Update** when you are done.

Tools > EdgeXOS Tools > SNMP/XGM Control

Enable to allow SNMP request to the EdgeXOS appliance, via port 161.



The XGM (XRoads Global Manager) is a server-based application which can be used to collect data from the EdgeXOS appliances. The RPM (Remote Provisioning Manager) module of the XGM system also provides the ability to automatically update the EdgeXOS appliance remotely and can be used to update multiple systems at the same time.



The XML Reporting Engine is designed to allow administrators to create their own detailed reports which can be completely customized. Additionally, these reports can be automatically generated in PDF format and emailed to any end-user. This functionality requires Microsoft Excel 2007 or later.

Link Control Configuration

Choose **Link Control** in the **Interfaces** tab **Interface Config** menu to open this page of configuration options.

Interfaces > Interface Config > Link Control

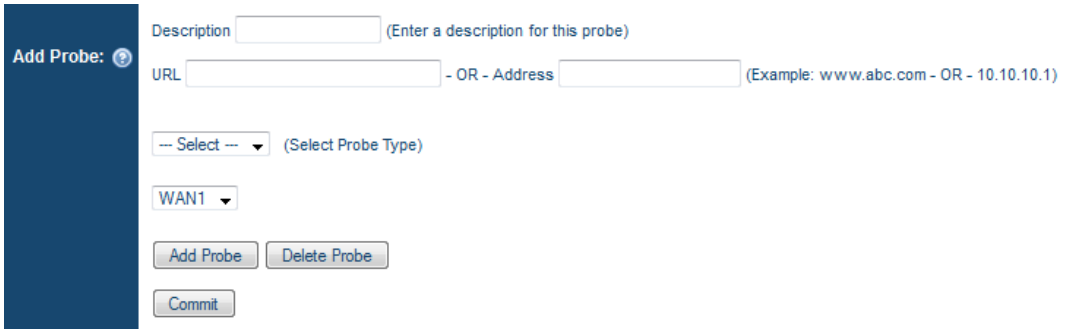
Use **Link Control** to determine how the appliance determines when and how to react to outages. The 'Holdtime' determines how long to wait, after an outage is detected, before link testing continues. This surpreses link flapping. The 'Link Test' addresses are what the EdgeXOS box uses to gather metric information for failover prediction. These addresses can be changed, however it is not recommended. NOTE: Only change these addresses if you have a specific network issue that requires changes.

Interfaces > Interface Config > Link Control

Probe Listing:

Select	Description	URL	Address	Probe	Interface
○				ICMP	wan1
○	A.ROOT-SERVERS.NET	a.root-servers.net		DNS	wan1
○	B.ROOT-SERVERS.NET	b.root-servers.net		DNS	wan2
○	C.ROOT-SERVERS.NET	c.root-servers.net		DNS	wan3
○	D.ROOT-SERVERS.NET	d.root-servers.net		DNS	wan4
○	F.ROOT-SERVERS.NET	f.root-servers.net		DNS	wan6
○	I.ROOT-SERVERS.NET	i.root-servers.net		DNS	wan5

Add probes which will be used after the default probing. These probes can be used to provide additional testing to remote sites in order to determine if an outage has occured.



When adding a new probe address, make sure to specify a description and select a probe type, either a URL or IP address can be entered for the test itself, if a URL is entered it will be translated in to an IP address during the testing procedure.

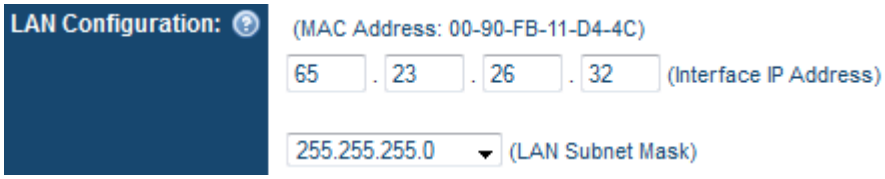
INTERFACE CONFIGURATION

LAN Interface Configuration

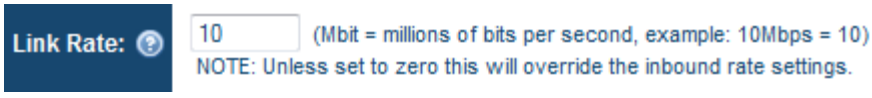
When configuring the LAN interface, keep in mind that any changes to this interface may result in losing access to the interface until your computers IP address is changed and the browser is directed to the newly changed address.

NOTE	The LAN interface does not need to be configured if WAN1 will be set to Proxy Mode. See the Proxy Mode Overview section for more information.
NOTE	Click **Apply** to apply changes, click **Reset** to return to previous configuration.

Interfaces > Interface Config > LAN Interface



This section allows you to administer the LAN network settings, including the IP Address and Subnet Mask configuration on the LAN interface. Make sure the IP Address consists of four octets, with each octet falling between a 0 and 255. Also provided is the MAC (Media Access Code, or hardware address) for the LAN Ethernet network adapter.

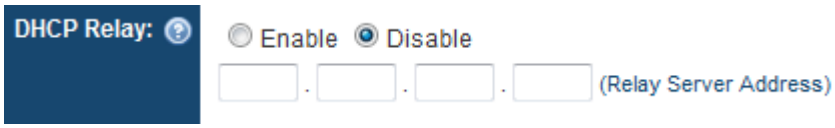

Link Rate:
10 (Mbit = millions of bits per second, example: 10Mbps = 10)
NOTE: Unless set to zero this will override the inbound rate settings.

Max Throughput for this WAN interface applies bi-directionally. This number is determined by both the hardware limitations of the unit, and the administrative settings provided by your Internet Service Provider.

Interfaces > Interface Config > LAN Interface

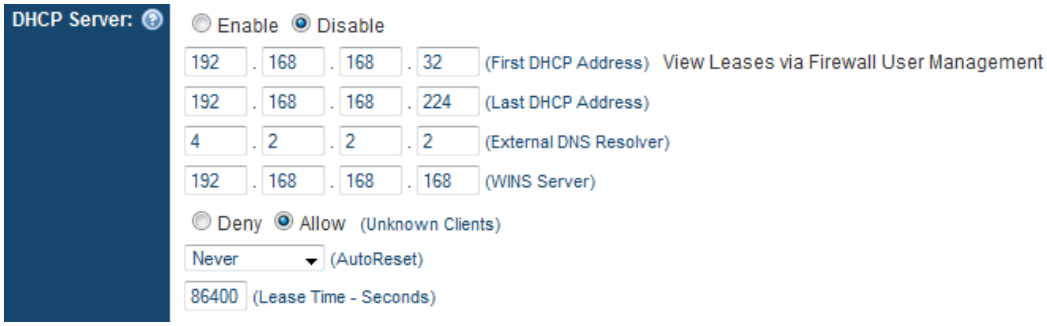
External DNS Resolvers:
4 . 2 . 2 . 2 (Primary DNS Server)
4 . 2 . 2 . 2 (Secondary DNS Server)
4 . 2 . 2 . 2 (Secondary DNS Server)
4 . 2 . 2 . 2 (Secondary DNS Server)
4 . 2 . 2 . 2 (Secondary DNS Server)
4 . 2 . 2 . 2 (Secondary DNS Server)
Disabled Enabled (Internal DNS Resolution, Zones Only)
Disabled Enabled (Recursive DNS Lookups)
Validate DNS (Make sure DNS is working, check Syslog report)

DNS resolvers are used to resolve domain names into IP addresses, this is used to make logs easier to read, and to enable the use of our RAC Management system, and to enable technical support using Internet names, instead of IP addresses. Please be sure to change at least the primary EdgeXOS DNS resolver so that name to IP resolution will work.



The DHCP Relay parameter enables you to pass DHCP broadcasts through the EdgeXOS appliance to a designated DHCP server. The relay cannot be used when the DHCP server is enabled or when any interface is set to use DHCP mode.

Interfaces > Interface Config > LAN Interface

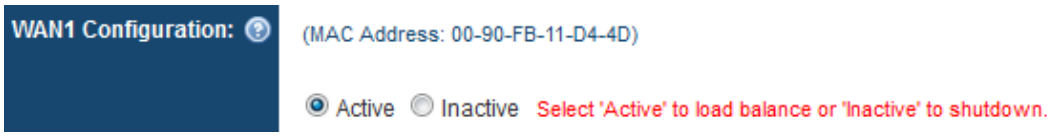

DHCP Server:
Enable
Disable
192 . 168 . 168 . 32 (First DHCP Address) View Leases via Firewall User Management
192 . 168 . 168 . 224 (Last DHCP Address)
4 . 2 . 2 . 2 (External DNS Resolver)
192 . 168 . 168 . 168 (WINS Server)
Deny
Allow (Unknown Clients)
Never (AutoReset)
86400 (Lease Time - Seconds)

The DHCP Server parameters enable you to configure the appliance's internal LAN DHCP server. DHCP (Dynamic Host Control Protocol) enables network devices and/or computers on the LAN network segment to obtain IP Addresses automatically from the appliance. This IP allocation is performed automatically thus simplifying client configuration. Be sure that the range specified is within the same address block as your LAN interface address or your clients will not be able to route through the appliance. It is recommended that you use the default lease time.

WAN Interface Configuration

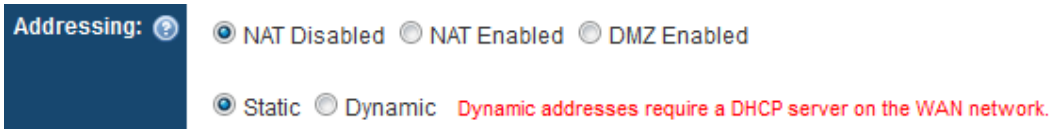
In order to configure the EdgeXOS appliance to access the Internet, the WAN interfaces must be configured. The following outlines the process for WAN configuration. Make sure that you have already determined which deployment method to use, as that is a critical step prior to actually configuring the WAN interfaces.

Interfaces > Interface Config > WAN Interface One



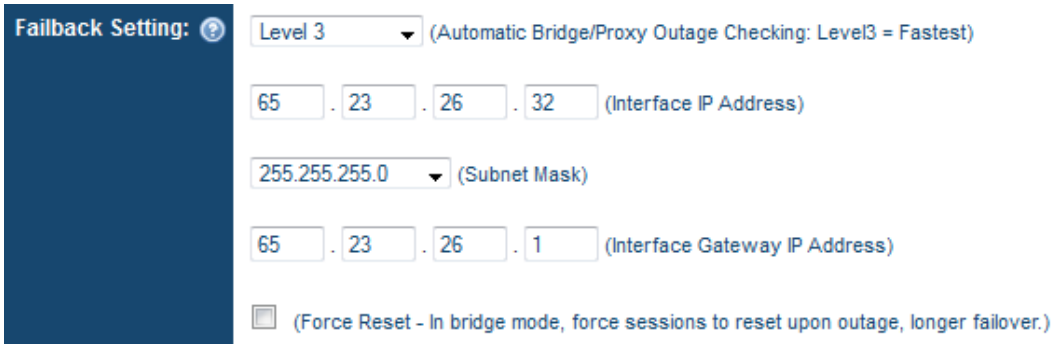
This section allows you to administer the WAN network settings, including the IP Address, Subnet Mask, and Gateway Address configuration on the WAN interface. Make sure the IP Address consists of four octets, with each octet falling between a 0 and 255. Also provided is the MAC (Media Access Code, or hardware address) for the WAN network adapter. You should be able to obtain all of this information from your Internet Service Provider.

The EdgeXOS appliance can be configured in one of three modes of operation. Bridge mode, which places the appliance in a true bridging state which passed all broadcasts between the LAN and WAN interfaces, it may require that you also add any secondary bridge networks via the Bridge Networks menu option under the Interfaces tab. Route/NAT mode, which allows the unit to route traffic (either statically or using NAT) between the LAN and WAN. Proxy mode, which is a pseudo bridging mode which allows for transparent insertion of the appliance between existing network devices without subnetting or changing existing IP network information (requires device reboots to clear ARP cache). NAT is the default mode of operation, however may customers with existing publically routed subnets use Bridge mode. Please reference to our QuickStart guide for configuration assistance.



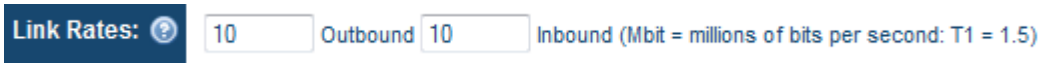
NAT or Network Address Translation enables a single IP address on your WAN network segment to be translated into hundreds of private IP addresses on your LAN network segment. This option must be enabled if 1) Your Internet Service Provider has only given you a single IP address, or 2) If you have already used a routed subnet via another WAN segment.

Interfaces > Interface Config > WAN Interface One


Failback Setting:
Level 3
(Automatic Bridge/Proxy Outage Checking: Level3 = Fastest)
65 . 23 . 26 . 32
(Interface IP Address)
255.255.255.0
(Subnet Mask)
65 . 23 . 26 . 1
(Interface Gateway IP Address)
(Force Reset - In bridge mode, force sessions to reset upon outage, longer failover.)

When in either bridge or proxy mode, the appliance takes the gateways IP address as it's LAN interface if the WAN1 link fails. When a failure does occur on the WAN1 interface when in either of these modes, the appliance will periodically test the WAN1 link. In proxy mode Level1 = Three checks per day, Level2 = Hourly checks, Level3 = Fifteen minute check. In Bridge mode Level1 = Hourly checks, Level2 = Five minute checks, Level3 = Fifteen second checks. Use this setting to determine how often the failback testing will occur. You can manually reset the interfaces at any time to force a failback.

The WAN Testing parameter determines how the EdgeXOS device will monitor the WAN connection. The EdgeXOS device monitors an Internet connection by testing the local gateway and the probe address. If the probe address should fail, the EdgeXOS device tests additional external Internet routers and server to determine if an outage has occurred (reference the Tools->Link Control section). If the Probe Address is left blank, the EdgeXOS device will attempt to find and automatically populate this address with the first hop beyond the broadband connection (once the Update button has been clicked). If this is unsuccesful, the address will need to be manually populated.



Max Throughput for this WAN interface applies bi-directionally. This number is determined by both the hardware limitations of the unit, and the administrative settings provided by your Internet Service Provider.

Interfaces > Interface Config > WAN Interface One

Weight is an administrative method for setting preference for a particular WAN network. The higher the weighted value the greater the preference for that particular WAN network. This effects how the appliance routes packets out to the Internet. The WAN interface with the highest weight will route most, if not all, of your network traffic.

Other Interface Configurations

- Static Routes
- Secondary IPs
- Secondary Bridges
- VLAN Tagging
- DHCP Groups

Static Routes

If your network has internal routes beyond an internal router or firewall, you may need to add static routes so that the EdgeXOS appliance know where to forward that traffic. Keep in mind, that the EdgeXOS platform only knows about its directly connected networks and the Internet (via its default 0.0.0.0 routes via active WAN links). All other routes must be specifically configured.

Interfaces > Interface Config > Static Routes

Static Routes: Static Routes enables you to configure statically assigned routes on your LAN network. The purpose for this feature is to allow companies with multiple network segments beyond the LAN segment to be routed appropriately. Most administrators will not need to worry about this feature.

Add Route: Add Static allows the administrator add a static route to the XRoads routing table. To add a static route, enter the network address (i.e. 10.10.10.1-254 = network address 10.10.10.0) and the subnet in slash notation (255.255.255.0 = 24) therefore the entry would be 10.0.0.0/24..

<< Back: Return to the LAN Interface page.

Add Route: Add a new static route.

Delete Route: Delete a static route.

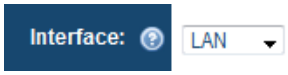
Secondary IPs

The EdgeXOS platforms support the assignment of multiple secondary IPs to each available Ethernet interface. These can be addresses within the same subnet as the primary or they can be within different subnets. The only limitation is that they cannot be from a subnet which is already associated with another interface.

Interfaces > Interface Config > Secondary IPs

Secondary network addresses enable the administrator to setup multiple networks on the LAN interface. This ensures that if a company has several non-consecutive network addresses that the XRoads EdgeXOS will still be able to route the networks appropriately.

Add Secondary allows the administrator to add secondary addresses to the interfaces. To add a secondary network to the LAN interface, enter the network address (i.e. 10.10.10.1-254 = network address 10.10.10.0) and the subnet in slash notation (255.255.255.0 = 24) therefore the entry would be 10.0.0.0/24. 24.



Use the drop down selection box to choose the interface you wish to view and/or configure.

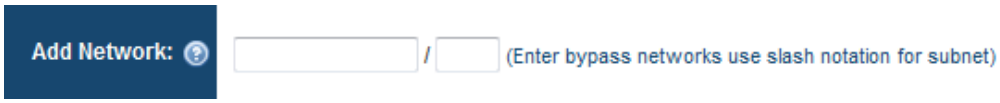
Secondary Bridges

When in bridge mode, use this to define additional networks to be associated with the LAN<->WAN1 bridge.

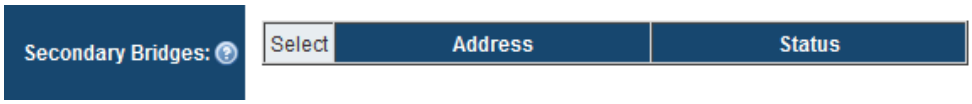
Interfaces > Interface Config > Secondary Bridges

Enter any networks which you wish to have bypass the appliance when in bridge mode. These networks will pass-through the appliance without being modified and/or shaped by the appliance.

Interfaces > Interface Config > Secondary Bridges



Enter any networks which you wish to have bypass the appliance when in bridge mode. These networks will pass-through the appliance without being modified and/or shaped by the appliance.



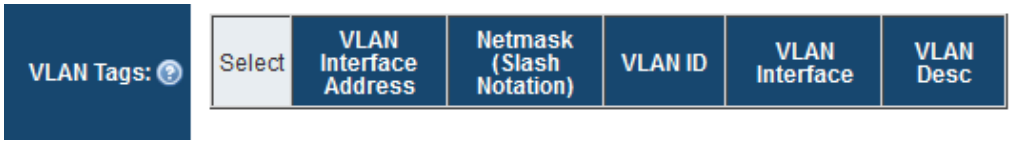
Enter any **additional** addresses that will be used on the WAN1 interface besides the gateway address. These addresses must reside within the primary WAN1 subnet.

Enter any additional addresses that will be used on the WAN1 interface besides the gateway address. These addresses must reside within the primary WAN1 subnet.

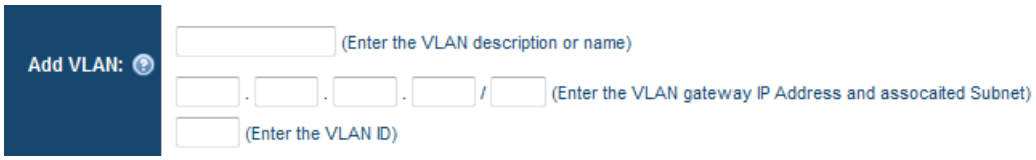
VLAN Tagging

Use this menu to configure VLANs within each EdgeXOS interface. The EdgeXOS platform does not bridge VLANs and thus any VLAN traffic passing through the EdgeXOS appliance must be terminated either by the appliance or have its tagging information stripped prior to the appliance.

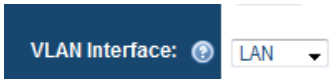
Interfaces > Interface Config > VLAN Tagging



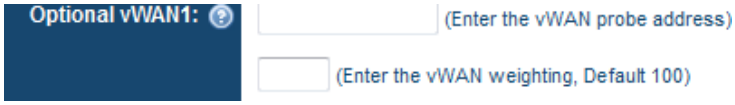
VLAN Tags: Connect the XRoads to the LAN network via VLAN tagging.



Define an IP address/network and VLAN ID for a specific VLAN which the XRoads will communicate with.



Use the drop down selection box to choose the interface you wish to view and/or configure.

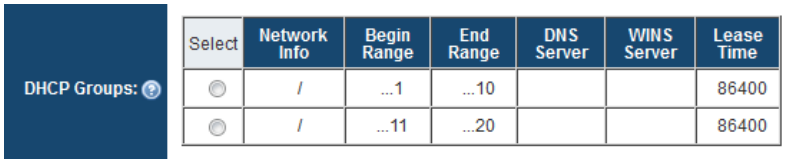


The optional vWAN parameters are for adding multiple bonding WAN interfaces to the WAN1 link. This is done via a VLAN switch connected to the WAN1 interface. Each vWAN interface can be used to scale the amount of bonded bandwidth via our MSA feature.

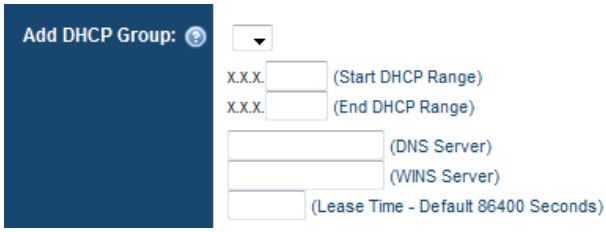
DHCP Groups

The EdgeXOS appliance supports multiple DHCP groups; these groups can be used to specify multiple DHCP ranges for each Ethernet interface. DHCP ranges cannot overlap and you cannot have more than one DHCP group per interface without being separated via a VLAN.

Interfaces > Interface Config > DHCP Groups



Use this section to add multipe DHCP domains which will typically be assigned from different VLAN networks and/or DMZ networks.



Enter the DHCP range (i.e. the forth octet, along with the DNS and WINS server (if any) with the amount of time which a specific lease should be allowed.

Application Routing Configuration

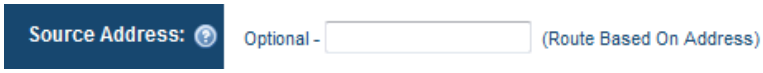
- Active DNS Policies
- Active Routing Policies
- Outbound Application Routing—Multi-Vector Priority (MVP) Routing
- Outbound Application Routing—Multi-Session Acceleration (MSA)
- Outbound Application Routing—MVP Best Path Routing
- Outbound Application Routing—MVP Application Routing

Add Service (MVP Application Routing)

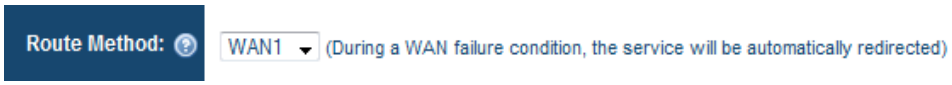
Used to determine the best interface to use for routing a specific application.

AppRouting > NetBalancing Selection > MVP Application Routing > Add Service

Service: Select one of the predefined services, or create a service by selecting a protocol and entering a port address.



Source Address: Enter a descriptive and unique name; this name will appear on all alerts, emails, etc.



Route Method: Select the interface you wish to use for this critical network, or select SMART for automatic WAN port selection based on the threshold and network statistics gathered from the Test Node. You may also select an optional gateway to use if more than one gateway exists on the WAN segments.

Reset: Reset previous configuration values.

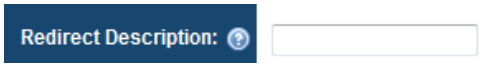
Add / Update: Add the new MVP application routing service.

View Services >>: Return to the main MVP Application Routing page.

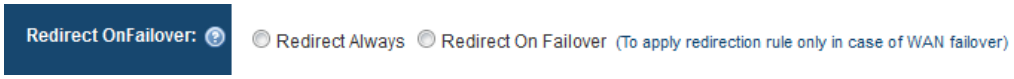
- Outbound Application Routing—MVP Redirect Routing

Add Redirect (MVP Redirect Routing)

AppRouting > NetBalancing Selection > MVP Redirect Routing > Add Redirect

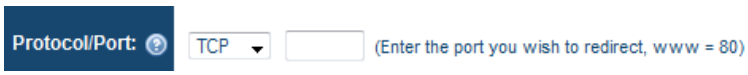


Redirect Description: Enter a descriptive and unique name; this name will appear on all alerts, emails, etc.



Redirect OnFailover: Select 'Always' or 'On Failover' based on when you wish to implement the redirection. For example, during a failure, all mail traffic will have to be redirected to a mail server which allows connections from the failover WAN address.

Redirect Address: Insert the address that you wish the traffic listed above to be redirected to.



Protocol/Port: Enter the port number (Example: web is TCP port 80) to be redirected. Select VOIP from the protocol drop-down to redirect all VoIP traffic to a specific server .

Reset: Reset previous configuration values.

Add / Update: Add the new MVP application routing service.

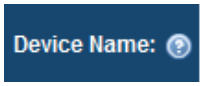
View Redirects >>: Return to the main MVP Redirect Routing page.

- In/Out Balancing Control—Vector Mappings

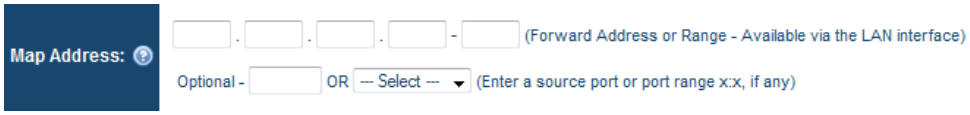
Add Service (In/Out Balancing Control Vector Mappings)

Used to add a vector map to an application or internal device.

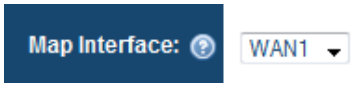
AppRouting > NetBalancing Selection > Vector Mappings > Add Service



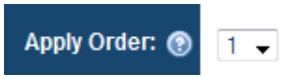
Device Name: Device Name allows you to identify a particular Vector mapping that you have created. It is generally recommended that you use a similar name as the DNS rule you created for this inbound load balancing device.


Map Address:
(Forward Address or Range - Available via the LAN interface)
Optional -
OR
--- Select ---
(Enter a source port or port range x:x, if any)

Map Address: The Map Address is the LAN address (and range of addresses) that are to be assigned to a particular WAN interface. Creating these mappings is required when the unit is in load balance mode AND has inbound traffic via either a proxy config on WAN1 or any advanced NAT mappings. When both of these conditions exist Vector Maps MUST be created. Optionally enter a source address in order to only force response traffic for a particular service and/or application back through the selected WAN interface. Enter VPN as the port number definition in order to specify any IPSec/PPTP VPN connection.



Map Interface: Select the WAN interface that will be used for mapping the internal address to an external gateway. This mapping MUST match your DNS rules in order for load balancing to work correctly.



Apply Order: The APPLY ORDER function is used to allow network administrators control which mappings will be applied and in which order based on the current active state of each WAN link. Only one server mapping can be active at any given time, thus the APPLY ORDER variable allows one to control which mapping will be used and to which WAN link it will be bound.

AppRouting > NetBalancing Selection > Vector Mappings > Add Service

Reset: Reset the rule's settings to their last saved state.

Add/Update: Add or update a firewall rules.

View Services>>: Return to the main Vector Mappings page.

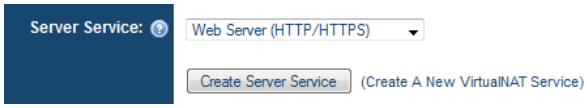
- Inbound Application Routing—Application Proxy (VNAT)

Add VirtualNAT Rule (Application Proxy)

Used to add a new Application Proxy rule.

AppRouting > NetBalancing Selection > Application Proxy > Add VirtualNAT Rule

Server Name: Enter the name of the server to which the defined service will be forwarded.



Server Service: Select the port which will be forward to the internal server. Multiple services can be defined by creating multiple VirtualNAT rules.

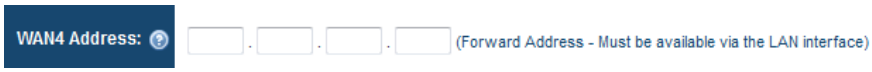
Internal Address: Enter the internal servers IP address. This address must be accessible via the EdgeXOS unit.

AppRouting > NetBalancing Selection > Application Proxy > Add VirtualNAT Rule

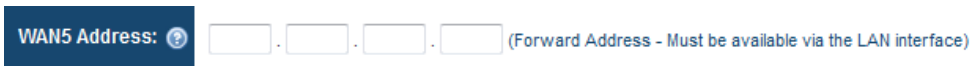
WAN 1 Address: This address will be added as a secondary address to the WAN1 interface. Once added, the service defined above will be forwarded to the defined Internal server address. When WAN1 is in proxy mode, this interface is not usable.

WAN 2 Address: This address will be added as a secondary address to the WAN2 interface. Once added, the service defined above will be forwarded to the defined Internal server address.

WAN 3 Address: This address will be added as a secondary address to the WAN3 interface. Once added, the service defined above will be forwarded to the defined Internal server address.



WAN 4 Address: This address will be added as a secondary address to the WAN4 interface. Once added, the service defined above will be forwarded to the defined Internal server address.



WAN 5 Address: This address will be added as a secondary address to the WAN5 interface. Once added, the service defined above will be forwarded to the defined Internal server address.

Reset: Reset the rule's settings to their last saved state.

Add/Update: Add or update a firewall rules.

View VirtualNAT Rules>>: Return to the main VirtualNAT Rules page.

- Inbound Application Routing—O2M NAT

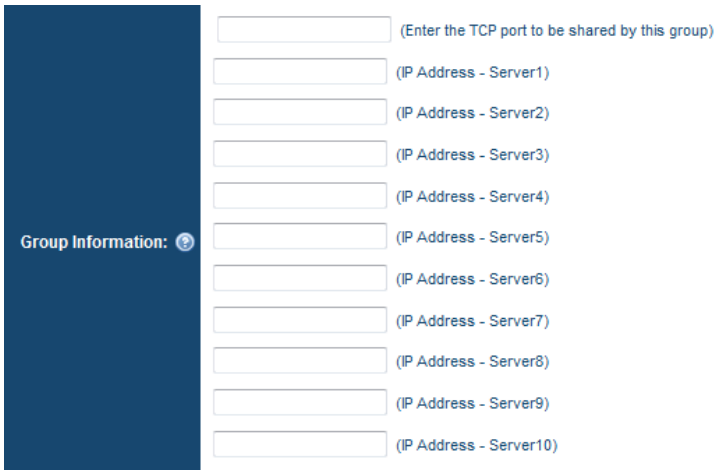
- Inbound Application Routing—O2O NAT
- Local Server Balancing—Server Load Balancing (SLB)

Add SLB Group

Create a new server load balancing rule.

AppRouting > NetBalancing Selection > Local Server Balancing > Add SLB Group

Server Group: Use the SLB module to balance traffic across two or more servers at the same time, thus improving server performance and reducing lag time for end-users. All connections are persistant.


Group Information:
(Enter the TCP port to be shared by this group)
(IP Address - Server1)
(IP Address - Server2)
(IP Address - Server3)
(IP Address - Server4)
(IP Address - Server5)
(IP Address - Server6)
(IP Address - Server7)
(IP Address - Server8)
(IP Address - Server9)
(IP Address - Server10)

Group Information: Enter the server group name, the TCP port to be used by the server group, and the IP addresses for each server in the group, up to a maximum of ten servers.

AppRouting > NetBalancing Selection > Local Server Balancing > Add SLB Group

Reset: Reset the rule's settings to their last saved state.

Add/Update: Add or update a firewall rules.

View Groups>>: Return to the main Server Load Balancing page.

- Private Link Bonding

Active DNS Policies

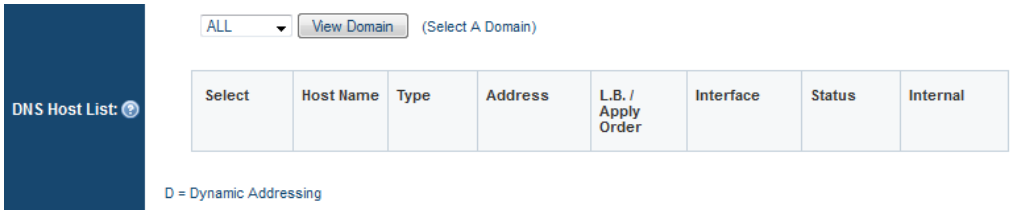
Active DNS Resolution: Enables inbound redundancy for services hosted on your LAN. Proper configuration is critical. Choose either:

- Domain Settings
- Host Records

Add Host Record

For a complete step-by-step guide to adding host records, please reference the How To Guide for ActiveDNS.

AppRouting > ActiveDNS Policies > ActiveDNS Resolution > Host Records > Add Record



DNS Host List: This listing contains all of the DNS records currently being served by this appliance. The Status field provides whether the record is ACTIVE or INACTIVE (meaning not currently being served by the ActiveDNS server). To delete a record, simply click the appropriate radio button and click the Delete button at the bottom of the page. To modify a record, click the appropriate radio button and click the Select button at the bottom of the page.

<< Add: Add a new host record.

Select: Select a host record.

Delete: Delete a host record

Verify: Verify a host record.

Save: Save changes.

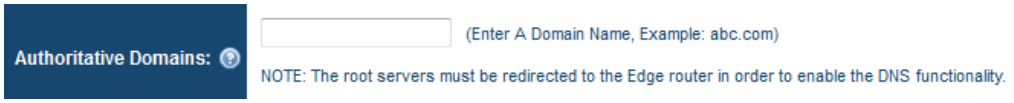
Delete All: Delete all configured host records.

- ActiveDNS-Geo

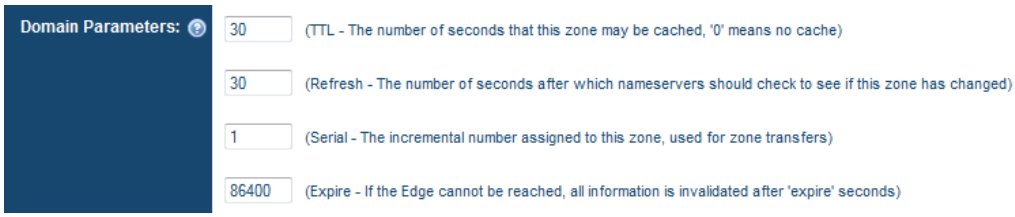
Domain Settings

Controls how the SOA records of the defined domains respond to other DNS servers.

AppRouting > ActiveDNS Policies > ActiveDNS Resolution > Domain Settings


Authoritative Domains:
(Enter A Domain Name, Example: abc.com)
NOTE: The root servers must be redirected to the Edge router in order to enable the DNS functionality.

Domain names controlled by the EdgeXOS unit, which creates both a primary and secondary NS server as well as the associated A records, for each domain. To enable authoritative DNS control on the hosted domains, contact the current registrar transfer the authoritative control to the addresses assigned to the EdgeXOS unit

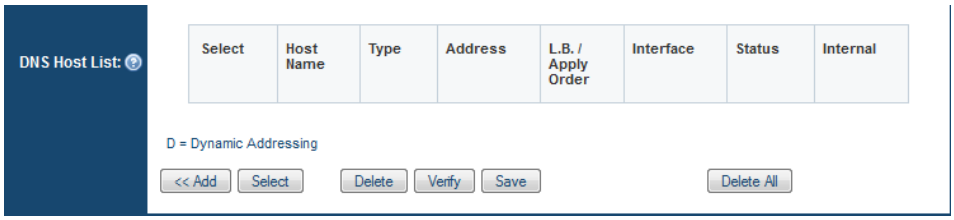

Domain Parameters:
30
(TTL - The number of seconds that this zone may be cached, '0' means no cache)
30
(Refresh - The number of seconds after which nameservers should check to see if this zone has changed)
1
(Serial - The incremental number assigned to this zone, used for zone transfers)
86400
(Expire - If the Edge cannot be reached, all information is invalidated after 'expire' seconds)

Use these setting to effect how this domain will be cached by other DNS servers. The TTL variable controls how long after a failure will the new information be obtained. The Refresh variable determines after what period of time the domain itself will be re-queried. The Expire variable determines after what period of time the domain information expires if the EdgeXOS device is no longer accessible.

Host Records

These are similar to host records in a standard DNS server.

AppRouting > ActiveDNS Policies > ActiveDNS Resolution > Host Records

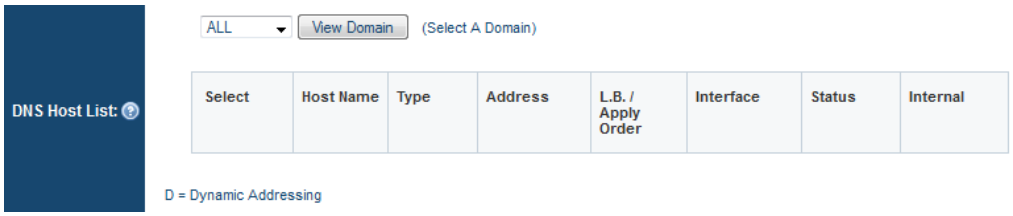


This listing contains all of the DNS records currently being served by this appliance. The Status field provides whether the record is ACTIVE or INACTIVE (meaning not currently being served by the ActiveDNS server). To delete a record, simply click the appropriate radio button and click the Delete button at the bottom of the page. To modify a record, click the appropriate radio button and click the Select button at the bottom of the page.

Add Host Record

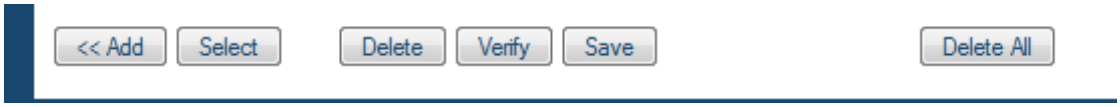
For a complete step-by-step guide to adding host records, please reference the How To Guide for ActiveDNS.

AppRouting > ActiveDNS Policies > ActiveDNS Resolution > Host Records > Add Record



DNS Host List: This listing contains all of the DNS records currently being served by this appliance. The Status field provides whether the record is ACTIVE or INACTIVE (meaning not currently being served by the ActiveDNS server). To delete a record, simply click the appropriate radio button and click the Delete button at the bottom of the page. To modify a record, click the appropriate radio button and click the Select button at the bottom of the page.

AppRouting > ActiveDNS Policies > ActiveDNS Resolution > Host Records > Add Record



<< Add: Add a new host record.

Select: Select a host record.

Delete: Delete a host record

Verify: Verify a host record.

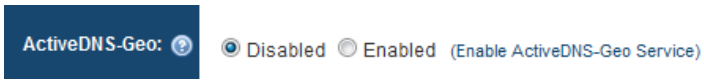
Save: Save changes.

Delete All: Delete all configured host records.

ActiveDNS-Geo

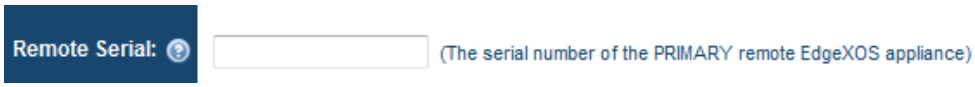
This feature enables two EdgeXOS platforms to work with each other when deployed at different geographic locations. One EdgeXOS is designated the primary and the one the secondary, the primary response for ALL domain information unless it fails, at which time the secondary takes over.

AppRouting > ActiveDNS Policies > ActiveDNS Resolution > ActiveDNS-Geo



Enable two geographically diverse EdgeXOS platforms to provide full DNS failover between sites. This helps ensures geographic server redundancy. It works by having the BACKUP EdgeXOS unit continuously probing the PRIMARY "remote" EdgeXOS unit to ensure that its DNS is responding. If the PRIMARY stops responding then the BACKUP appliance will take over. Only configure this service on the BACKUP EdgeXOS unit.

AppRouting > ActiveDNS Policies > ActiveDNS Resolution > ActiveDNS-Geo



The serial number of the PRIMARY EdgeXOS platform. Only enable this service on the BACKUP EdgeXOS unit, not the PRIMARY.

WAN Addresses: The WAN IP addresses of the PRIMARY EdgeXOS unit. Only activate this service on the BACKUP EdgeXOS unit.

Active Routing Policies

This screen shows all of the active route policies configured within the appliance.

Choose **Active Routing Policies** in the **AppRouting** tab **NetBalancing Selection** menu to open this page of configuration options.

AppRouting > NetBalancing Selection > Active Routing Policies

Vector Routes:

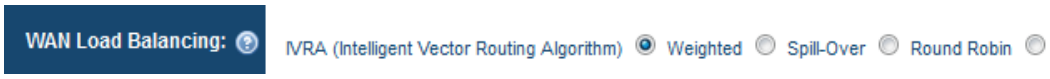
Service Name	Interface	External Addr	External Port	Internal Addr	Internal Port	VNAT	Vector Route
Exchange	WAN1	216.119.234.54	ANY:ANY	192.0.0.43			VR->
Exchange	WAN2	216.119.234.3	ANY:ANY	192.0.0.3			VR->
Exchange	WAN3	216.119.234.32	ANY:ANY	192.0.0.3			VR->
Exchange	WAN3	OUTBOUND		192.0.0.3			<--VR
web	WAN1	OUTBOUND	8080:8085	10.10.1.1			<--VR

This list contains all of the administratively applied servers / services. When deleting a selection the two options are Partial Delete and Full Delete, full delete will also remove any secondary addresses added to the WAN interface. This will also cause a momentary loss of network connectivity. To ensure session connectivity only use Partial Delete during normal operating hours and reboot the unit during your next maintanence period to remove any unwanted secondary addresses.

Outbound Application Routing—Multi-Vector Priority (MVP) Routing

Choose **Multi-Vector Priority (MVP) Routing** in the **AppRouting** tab **NetBalancing Selection** menu to open this page of configuration options.

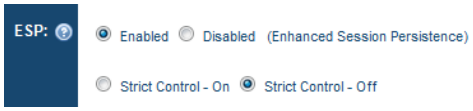
AppRouting > NetBalancing Selection > Multi-Vector Priotity (MVP) Routing



Network load balancing is enabled through the division of network sessions across two or more Internet connections. The applications below which are enabled are load balanced across the ACTIVE WAN connections. Load balancing is performed by routing each unique session across the different interfaces based on the weighting associated with each connection. Weighting is affected by multiple factors, including the administratively assigned weighting and interface usage.

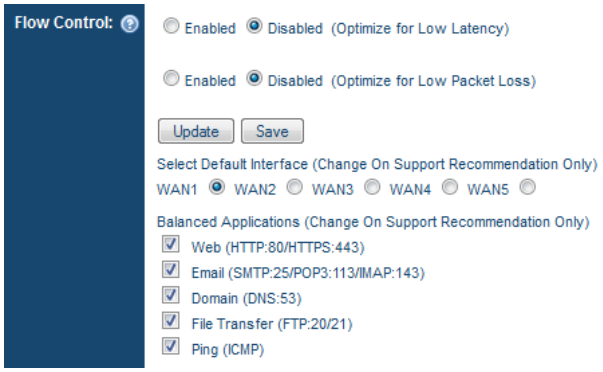
Custom applications can be configured by entering the application protocol and port information below.

NOTE: Session load balancing is NOT the same as network bonding, which requires devices at both ends of the connection to disassemble and reassemble the packet streams and cannot be used for general Internet traffic. Session based load balancing, will not increase per session throughput (i.e. individual speed tests will not show an increase), however it does increase network throughput by dividing session requests between the multiple ACTIVE WAN interfaces, therefore web sites and other multi-session applications will show an increase in download speeds.



Tracks sessions in real-time and will automatically ensure that each session maintains its "stickiness" to a specific WAN link once the session has been initiated.

AppRouting > NetBalancing Selection > Multi-Vector Priotity (MVP) Routing



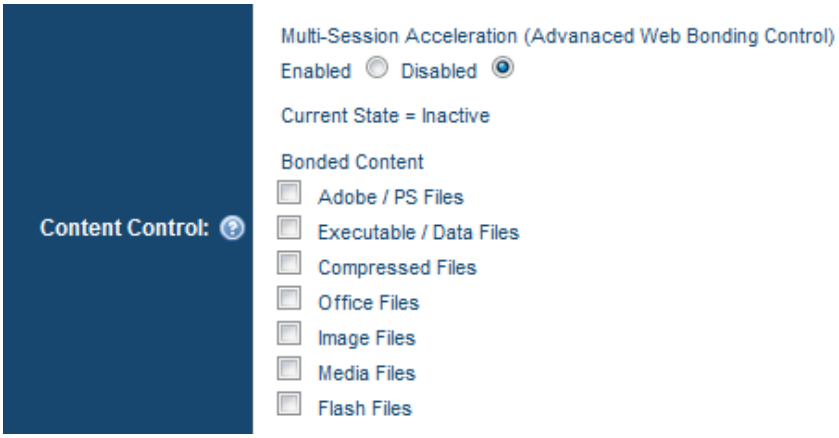
Enable low latency if you have determined that your ISP's deliver lower latency to the Internet, i.e. under 60ms on average. Enable low packet loss if you have determined that your ISP's do not have high packet loss, i.e. no dropped packets over long periods of time. You can use MVP Best Path Routing w/SLA reporting to determine how well your ISP's are performing and then change these settings accordingly.

Outbound Application Routing—Multi-Session Acceleration (MSA)

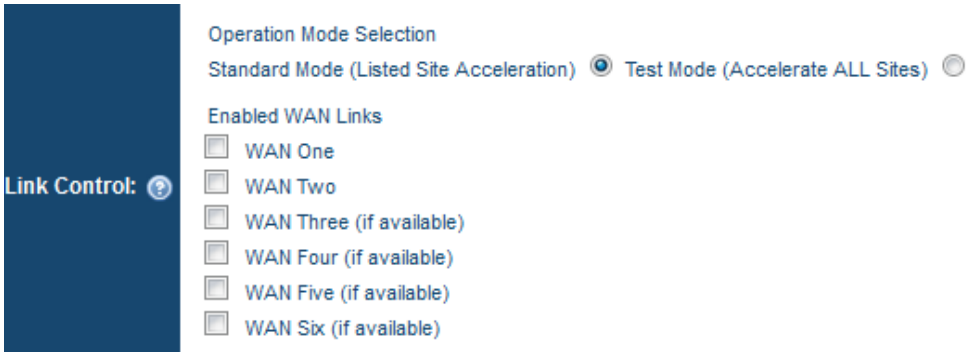
Used to determine how applications will be routed across the various links.

In the case of MSA, these settings are used to determine how traffic is bonded across the selected links for faster downloads and accelerated throughput between multiple ISP connections.

AppRouting > NetBalancing Selection > Multi-Session Acceleration (MSA)



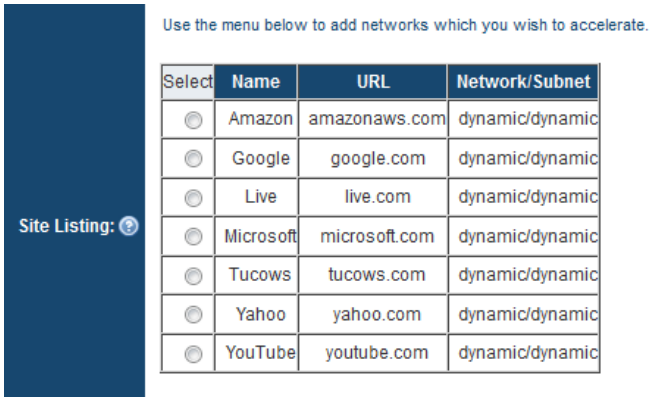
Multi-Session Web Acceleration is a unique ability found in the EdgeXOS platform which can increase the download speed of certain files which are web-accessible via two or more Internet links. When enabled our multisession technology will automatically detect when certain files types are being downloaded, based on this configuration and automatically accelerate the download of those files.



Enable those interfaces which you wish to utilize with the MSA bandwidth bonding feature set.

AppRouting > NetBalancing Selection > Multi-Session Acceleration (MSA)

DNS resolvers are used to resolve domain names into IP addresses, this is used to make logs easier to read, and to enable the use of our RAC Management system, and to enable technical support using Internet names, instead of IP addresses. Please be sure to change at least the primary EdgeXOS DNS resolver so that name to IP resolution will work.



Define which web sites to accelerate by the MSA module. Customers that experience heavy load conditions may wish to minimize which sites are accelerated in order to reduce load, this can be accomplished by using per site filtering controls.

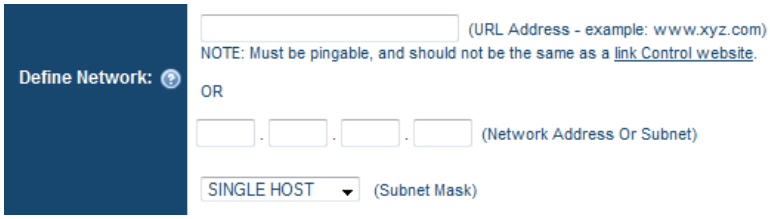
Enter the URL for the site, the IP network for the site, example 10.20.30.0, and the subnet in slash notation, example 24.

Outbound Application Routing—MVP Best Path Routing

Determines the best path for a specifically defined URL and/or network range.

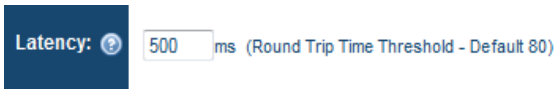
AppRouting > NetBalancing Selection > MVP Best Path Routing

Route Description: Enter a descriptive and unique name; this name will appear on all alerts, emails, etc.


Define Network:
(URL Address - example: www.xyz.com)
NOTE: Must be pingable, and should not be the same as a link Control website.
OR
(Network Address Or Subnet)
SINGLE HOST
(Subnet Mask)

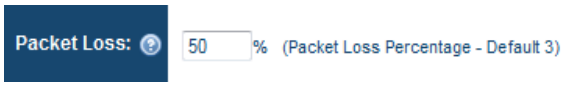
Define Network: Enter the network address and subnet mask for the critical network you wish to monitor. Example: 4.2.2.0 255.255.255.0

Test Node: Enter the specific address that will be used to obtain network statistics for this critical network. Make sure to use an address that is within the range specified in the network definition above.

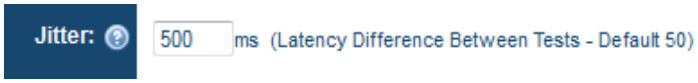


Latency: Enter the thresholds to be used for determining when the route should be changed based on the statistics gathered via the Test Node.

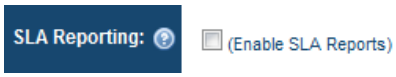
AppRouting > NetBalancing Selection > MVP Best Path Routing



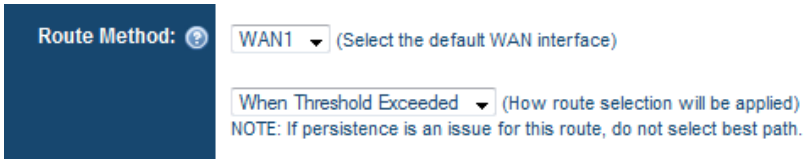
Packet Loss: Enter the thresholds to be used for determining when the route should be changed based on the statistics gathered via the Test Node.



Jitter: Enter the thresholds to be used for determining when the route should be changed based on the statistics gathered via the Test Node.



SLA Reporting: Creates graphical and statistical reporting for the Best Path Route. This data is found under the reporting tab.

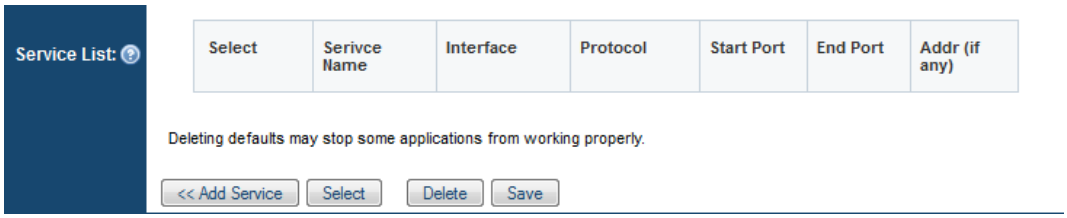

Route Method:
WAN1
(Select the default WAN interface)
When Threshold Exceeded
(How route selection will be applied)
NOTE: If persistence is an issue for this route, do not select best path.

Route Method: Select the interface you wish to use for this critical network, or select SMART for automatic WAN port selection based on the threshold and network statistics gathered from the Test Node. You may also select an optional gateway to use if more than one gateway exists on the WAN segments.

Outbound Application Routing—MVP Application Routing

TBW. See also Add Service (MVP Application Routing).

AppRouting > NetBalancing Selection > MVP Application Routing

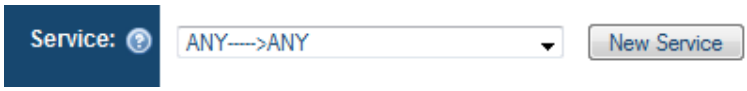


This list contains all of the administratively applied EdgeXOS routing rules.

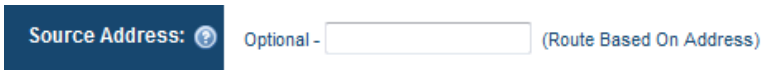
Add Service (MVP Application Routing)

Used to determine the best interface to use for routing a specific application.

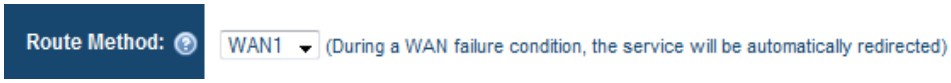
AppRouting > NetBalancing Selection > MVP Application Routing > Add Service



Service: Select one of the predefined services, or create a service by selecting a protocol and entering a port address.



Source Address: Enter a descriptive and unique name; this name will appear on all alerts, emails, etc.



Route Method: Select the interface you wish to use for this critical network, or select SMART for automatic WAN port selection based on the threshold and network statistics gathered from the Test Node. You may also select an optional gateway to use if more than one gateway exists on the WAN segments.

AppRouting > NetBalancing Selection > MVP Application Routing > Add Service

Reset: Reset previous configuration values.

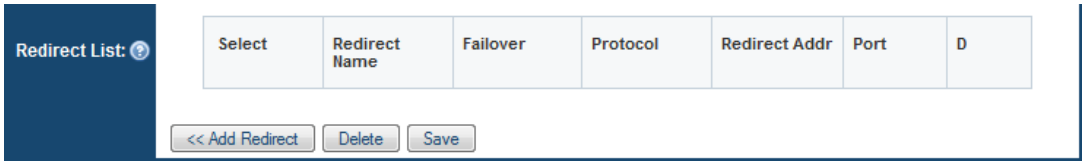
Add / Update: Add the new MVP application routing service.

View Services >>: Return to the main MVP Application Routing page.

Outbound Application Routing—MVP Redirect Routing

Used to re-route an application upon the determination of a network failure, beyond the default behavior which is to route via the next available path.

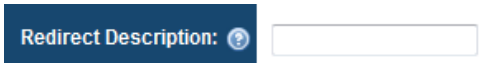
AppRouting > NetBalancing Selection > MVP Redirect Routing Opions



This list contains all of the administratively applied EdgeXOS routing rules.

Add Redirect (MVP Redirect Routing)

AppRouting > NetBalancing Selection > MVP Redirect Routing > Add Redirect

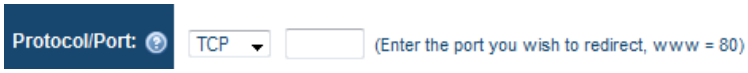


Redirect Description: Enter a descriptive and unique name; this name will appear on all alerts, emails, etc.

AppRouting > NetBalancing Selection > MVP Redirect Routing > Add Redirect

Redirect OnFailover: Select 'Always' or 'On Failover' based on when you wish to implement the redirection. For example, during a failure, all mail traffic will have to be redirected to a mail server which allows connections from the failover WAN address.

Redirect Address: Insert the address that you wish the traffic listed above to be redirected to.



Protocol/Port: Enter the port number (Example: web is TCP port 80) to be redirected. Select VOIP from the protocol drop-down to redirect all VoIP traffic to a specific server .

Reset: Reset previous configuration values.

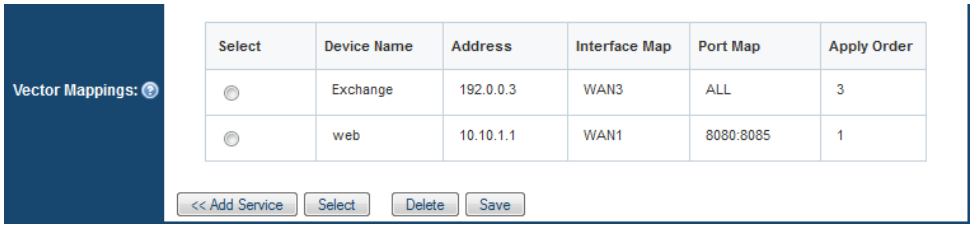
Add / Update: Add the new MVP application routing service.

View Redirects >>: Return to the main MVP Redirect Routing page.

In/Out Balancing Control—Vector Mappings

Used to ensure that sessions originating on one link stay routed across that same link. Vector Mappings can be applied to internal device to force it out a specific WAN link, or can be applied based on a specific inbound service to ensure that the outbound traffic used the same link that was used for the inbound traffic. This ensures session persistence for server applications.

AppRouting > NetBalancing Selection > Vector Mappings



Vector Mappings: This list contains all of the administratively applied EdgeXOS routing rules.

Add Service (In/Out Balancing Control Vector Mappings)

Used to add a vector map to an application or internal device.

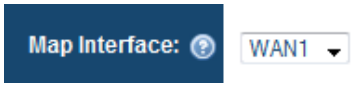
AppRouting > NetBalancing Selection > Vector Mappings > Add Service

Device Name: Device Name allows you to identify a particular Vector mapping that you have created. It is generally recommended that you use a similar name as the DNS rule you created for this inbound load balancing device.

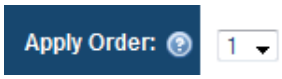
Map Address:
(Forward Address or Range - Available via the LAN interface)
Optional -
OR
--- Select ---
(Enter a source port or port range x:x, if any)

Map Address: The Map Address is the LAN address (and range of addresses) that are to be assigned to a particular WAN interface. Creating these mappings is required when the unit is in load balance mode AND has inbound traffic via either a proxy config on WAN1 or any advanced NAT mappings. When both of these conditions exist Vector Maps MUST be created. Optionally enter a source address in order to only force response traffic for a particular service and/or application back through the selected WAN interface. Enter VPN as the port number definition in order to specify any IPSec/PPTP VPN connection.

AppRouting > NetBalancing Selection > Vector Mappings > Add Service



Map Interface: Select the WAN interface that will be used for mapping the internal address to an external gateway. This mapping MUST match your DNS rules in order for load balancing to work correctly.



Apply Order: The APPLY ORDER function is used to allow network administrators control which mappings will be applied and in which order based on the current active state of each WAN link. Only one server mapping can be active at any given time, thus the APPLY ORDER variable allows one to control which mapping will be used and to which WAN link it will be bound.

Reset: Reset the rule's settings to their last saved state.

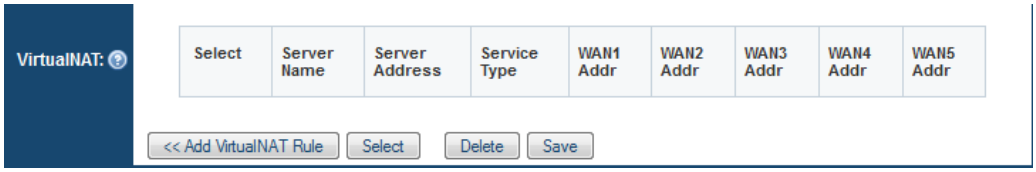
Add/Update: Add or update a firewall rules.

View Services>>: Return to the main Vector Mappings page.

Inbound Application Routing—Application Proxy (VNAT)

The Application Proxy enables users to setup inbound load balancing and failover of applications connecting to an internal resource. The Application Proxy should be the default method for enabling inbound web server, email server, and other server access from the Internet across multiple WAN links. See also Add VirtualNAT Rule (Application Proxy).

AppRouting > NetBalancing Selection > Application Proxy (VNAT)



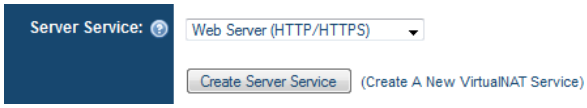
This is a list of the VirtualNAT servers which have been configured. These rules are currently in effect.

Add VirtualNAT Rule (Application Proxy)

Used to add a new Application Proxy rule.

AppRouting > NetBalancing Selection > Application Proxy > Add VirtualNAT Rule

Server Name: Enter the name of the server to which the defined service will be forwarded.



Server Service: Select the port which will be forward to the internal server. Multiple services can be defined by creating multiple VirtualNAT rules.

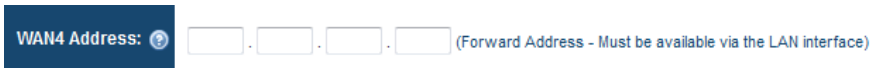
Internal Address: Enter the internal servers IP address. This address must be accessible via the EdgeXOS unit.

AppRouting > NetBalancing Selection > Application Proxy > Add VirtualNAT Rule

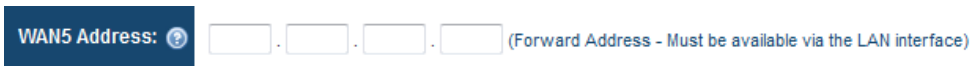
WAN 1 Address: This address will be added as a secondary address to the WAN1 interface. Once added, the service defined above will be forwarded to the defined Internal server address. When WAN1 is in proxy mode, this interface is not usable.

WAN 2 Address: This address will be added as a secondary address to the WAN2 interface. Once added, the service defined above will be forwarded to the defined Internal server address.

WAN 3 Address: This address will be added as a secondary address to the WAN3 interface. Once added, the service defined above will be forwarded to the defined Internal server address.



WAN 4 Address: This address will be added as a secondary address to the WAN4 interface. Once added, the service defined above will be forwarded to the defined Internal server address.



WAN 5 Address: This address will be added as a secondary address to the WAN5 interface. Once added, the service defined above will be forwarded to the defined Internal server address.

Reset: Reset the rule's settings to their last saved state.

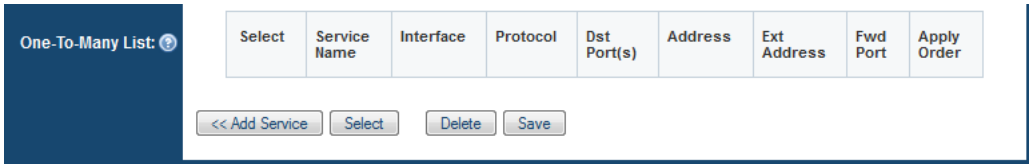
Add/Update: Add or update a firewall rules.

View VirtualNAT Rules>>: Return to the main VirtualNAT Rules page.

Inbound Application Routing—O2M NAT

Used to create a NAT rule for mapping a single external address to multiple internal addresses using different ports.

AppRouting > NetBalancing Selection > O2M NAT



This list contains all of the administratively applied servers / services. When deleting a selection the two options are Partial Delete and Full Delete, full delete will also remove any secondary addresses added to the WAN interface. This will also cause a momentary loss of network connectivity. To ensure session connectivity only use Partial Delete during normal operating hours and reboot the unit during your next maintanence period to remove any unwanted secondary addresses.

Inbound Application Routing—O2O NAT

Used to create a NAT rule for mapping a single external address to a single internal addresses, all ports are mapped to the internal address.

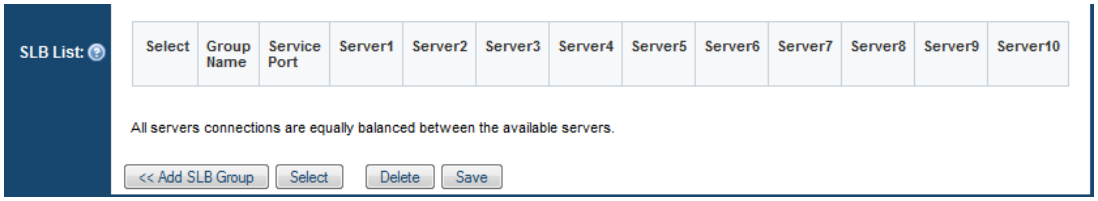
AppRouting > NetBalancing Selection > O2O NAT

This list contains all of the administratively applied servers / services. When deleting a selection the two options are Partial Delete and Full Delete, full delete will also remove any secondary addresses added to the WAN interface. This will also cause a momentary loss of network connectivity. To ensure session connectivity only use Partial Delete during normal operating hours and reboot the unit during your next maintanence period to remove any unwanted secondary addresses.

Local Server Balancing—Server Load Balancing (SLB)

Use this service to setup server balancing, i.e. a inbound client requests can be balanced across two or more internal servers.

AppRouting > NetBalancing Selection > Local Server Balancing



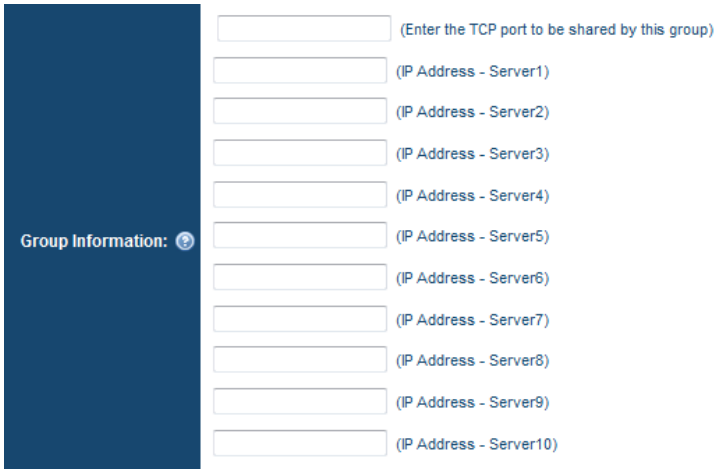
SLB List: This is a list of server load balancing groups.

Add SLB Group

Create a new server load balancing rule.

AppRouting > NetBalancing Selection > Local Server Balancing > Add SLB Group

Server Group: Use the SLB module to balance traffic across two or more servers at the same time, thus improving server performance and reducing lag time for end-users. All connections are persistant.


Group Information:
(Enter the TCP port to be shared by this group)
(IP Address - Server1)
(IP Address - Server2)
(IP Address - Server3)
(IP Address - Server4)
(IP Address - Server5)
(IP Address - Server6)
(IP Address - Server7)
(IP Address - Server8)
(IP Address - Server9)
(IP Address - Server10)

Group Information: Enter the server group name, the TCP port to be used by the server group, and the IP addresses for each server in the group, up to a maximum of ten servers.

Reset: Reset the rule's settings to their last saved state.

Add/Update: Add or update a firewall rules.

View Groups>>: Return to the main Server Load Balancing page.

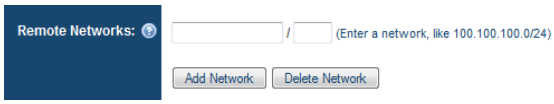
Private Link Bonding

This feature allows administrates to bond two or more private WAN links, i.e. you wish to combine two T1 connections, both going to the same location, but would like to fully

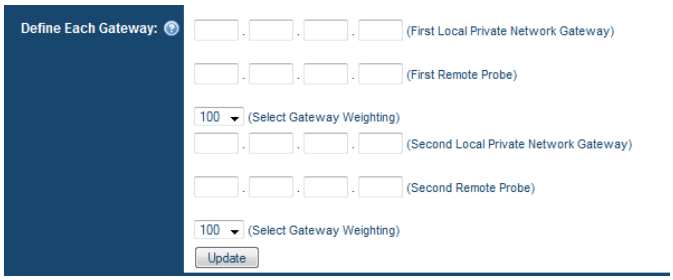
utilize the bandwidth of each link. Private link bonding performs this bonding via Layer-3 between the two sites.

AppRouting > NetBalancing Selection > Private Link Bonding

Private Network Balancing: This feature is currently in BETA development and will be used to allow two appliances at a single location to wrk with two appliances at a remote location in order to establish connectivity between the two locations across both a public and private connection.



Remote Networks: ESP Pass-Through is designed to allow for certain networks to be accessible without using enhanced session routing. Simply enter the network and subnet that should be bypassed.



Define Each Gateway: Define the remote network gateway across the private WAN link. Then define the probe address to test to for determining the status of this route. Then apply the weighting for this route. Next define the remote network gateway for either a) the second private WAN link, or b) the second local EdgeXOS appliance to which this device will forward traffic for distribution across one more multiple Internet (or non-private) WAN links. This requires two EdgeXOS appliances at each site. Then configure the probe address for this second network and assign a weight.

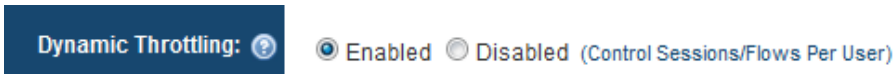
Application Shaping Configuration

- **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**
- **Error! Reference source not found.**

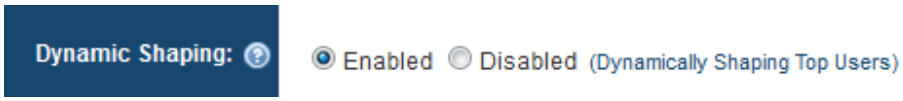
Dynamic Bandwidth Management

The ability to automatically adjust bandwidth flows in order to throttle abusive traffic. DBM can be used to reduce P2P and other recreational traffic in order to ensure that no individual or group of users is able to utilize all of the available bandwidth.

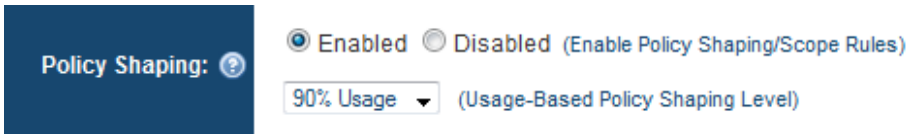
AppShaping > EdgeXOS Routing > Dynamic Bandwidth Management



Control how many sessions are allowed per host per second. This reduces end-users ability to utilize P2P and other similar applications which open large of sessions in order to use as much bandwidth as possible for downloads.



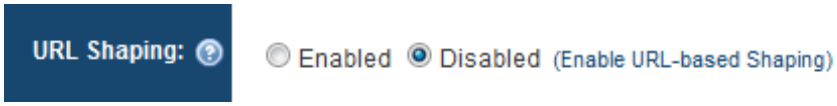
This feature ensures that all users/devices maintain equal access to the networks bandwidth. With this service enabled no single user/device is able to monopolize the bandwidth. Bandwidth is evenly distributed between each user so that no one user/device is able to slow down the down for other users/devices. This service can be used in conjunction with policy-based or application-based shaping.



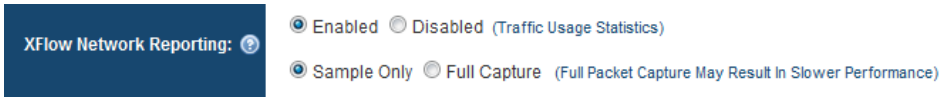
Policy shaping allows network administrators to set very specific in-flow and out-flow rates for specific applications and/or hosts. Shaping policies can be based on IP address, port, protocol, src/dst or any combination and can be assigned based on group or individually. Rate settings allow users to be throttled to specific minimum and maximum limits with the ability to burst, additionally each group excepts up to 12 different priority levels.

AppShaping > EdgeXOS Routing > Dynamic Bandwidth Management

Used to prioritize specific applications over others, for example setting a higher priority for https applications while lowering priority for email applications.



Used to prioritize specific URL's over others, for example setting a higher priority for business critical web applications while lowering priority for streaming sites.

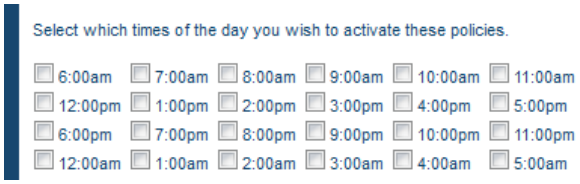


The XFLOW network reporting module provides application and end-user reporting. XFlow works by sampling network usage over time in order to determine top users and applications. XFlow may also perform full packet capture which provides greater detail and more accurate information, however at times this level of data collection can be processor intensive, thus the administrator has the ability to disable these collection tasks in order to improve traffic throughput when under heavy load conditions.

DBM Session Throttling

Uses to prevent end-users, as defined, from starting more than the allocated number of sessions per sessions per second, and can be further used to prevent end-users from passing more than the specified number of packets per second.

AppShaping > EdgeXOS Routing > DBM Session Throttling


Select which times of the day you wish to activate these policies.
6:00am 7:00am 8:00am 9:00am 10:00am 11:00am
12:00pm 1:00pm 2:00pm 3:00pm 4:00pm 5:00pm
6:00pm 7:00pm 8:00pm 9:00pm 10:00pm 11:00pm
12:00am 1:00am 2:00am 3:00am 4:00am 5:00am

Time checkboxes: Select which times of the day you wish to activate these policies.

When enabled dynamic throttling will only be enabled when utilization goes above the Usage-Based Policy Shaping Level set under the DBM control menu. Leave disabled if you want the throttling enabled all of the time. Enable if you only want throttling to turn on during period of high utilization.

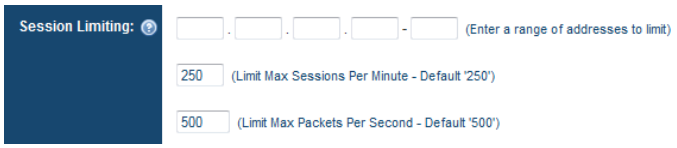
When enabled the system will apply both session limits as well as per packet controls on those IP addresses which are defined. Throttling occurs when the number of packets per second for a user exceeds what has been allocated.

This is a list of the session limiting address ranges. Limits will be applied to these ranges in order to reduce the number of sessions which any individual address will be able to create each second.

Add Range (DBM Session Throttling)

Create a new throttling rule.

AppShaping > EdgeXOS Routing > DBM Session Throttling > Add Range


Session Limiting:
(Enter a range of addresses to limit)
250
(Limit Max Sessions Per Minute - Default '250')
500
(Limit Max Packets Per Second - Default '500')

Session Limiting: Session limiting and Packet Limiting enable network administrators to set specific limits for bandwidth usage on a per IP basis. These limitations work well in environments where strict controls are necessary during periods throughout the day. Note: Enabling this feature can add latency on large networks.

Add Range: Add the new DBM session throttling range.

Range List >>: Return to the main DBM Session Throttling page.

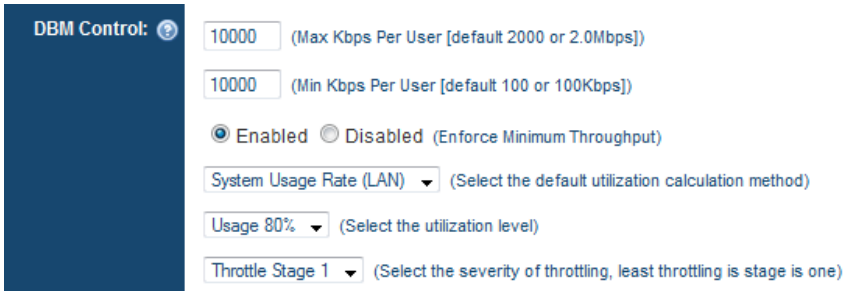
DBM Adaptive Shaping

Create a new DBM rule.

AppShaping > EdgeXOS Routing > DBM Adaptive Shaping

Time Options: Select time properties.

AppShaping > EdgeXOS Routing > DBM Adaptive Shaping

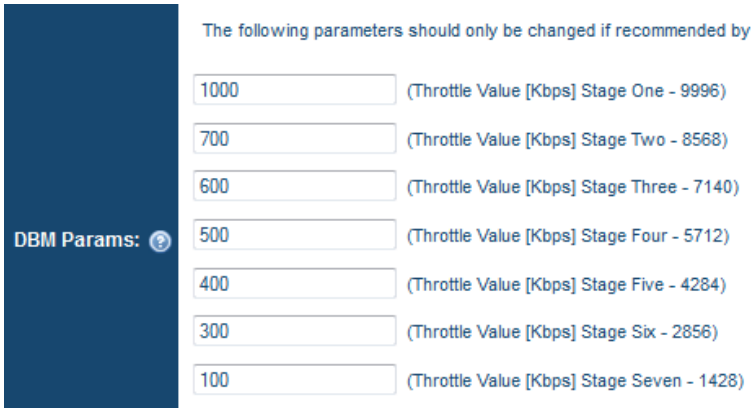


DBM Control: This feature ensures that all users/devices maintain equal access to the networks bandwidth. With this service enabled no single user/device is able to monopolize the bandwidth. Bandwidth is evenly distributed between each user so that no one user/device is able to slow down the down for other users/devices. This service can be used in conjunction with policy-based or application-based shaping.

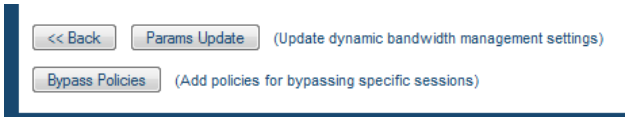
Advanced Params (DBM Adaptive Shaping)

If you wish to specify the specific throttle speeds at each level, you can specify those entries here:

AppShaping > EdgeXOS Routing > DBM Adaptive Shaping > Advanced Params


DBM Params:
The following parameters should only be changed if recommended by support.
1000 (Throttle Value [Kbps] Stage One - 9996)
700 (Throttle Value [Kbps] Stage Two - 8568)
600 (Throttle Value [Kbps] Stage Three - 7140)
500 (Throttle Value [Kbps] Stage Four - 5712)
400 (Throttle Value [Kbps] Stage Five - 4284)
300 (Throttle Value [Kbps] Stage Six - 2856)
100 (Throttle Value [Kbps] Stage Seven - 1428)

DBM Params: These parameters should only be modified if you understand how these modifications will effect the shaping of this device. These numbers should represent a ratio between the inbound and outbound throughput rates and how traffic is throttled. Use the following examples to understand how the ratio works. Example: If the outbound rate is 10000 or 10Mbps, then the stage ratios are as follows, Stage 1 = 400, Stage 2 = 320, Stage 3 = 266, Stage 4 = 150, Stage 5 = 100, Stage 6 = 53 Stage 7 = 32. The penalty is how long in seconds that a specific throttle policy will stay in place once implemented without changing, the holdtime is how long in seconds that the system will wait between throttle updates.



<< Back: Return to the main DBM Adaptive Shaping page.

Params Update: Update dynamic bandwidth management settings.

Bypass Policies: Add policies for bypassing specific sessions. See

Bypass Policies (DBM Adaptive Shaping)

These rules allow specific end-users to bypass the DBM rules and not be throttled automatically as other users would be.

AppShaping > EdgeXOS Routing > DBM Adaptive Shaping > Bypass Policies

Bypass Policy: Use this function to allow certain internal hosts/servers or external websites to bypass the content filtering system. Any address/network entered here will not be filtered. Use to allow servers through the filter, or specific end-users, or if you are having problems with a specific website, ping the site to obtain its IP address/network and enter it here.

<< DBM Control: Return to the main DBM Adaptive Shaping page.

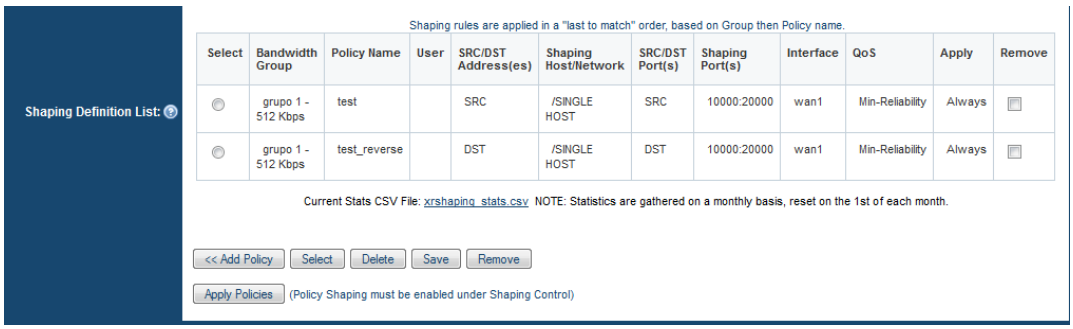
Bypass Add / Update: Update dynamic bandwidth management settings.

View Bypass List: Add policies for bypassing specific sessions.

Policy-Based Shaping

This allows administrates to create very specific and granular shaping rules in order to either guarantee bandwidth or limit bandwidth for a specific server, end-user or group of users.

AppShaping > EdgeXOS Routing > Policy-Based Shaping

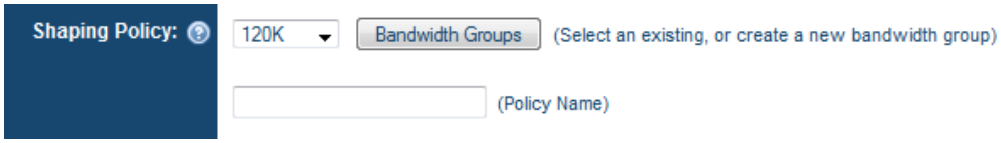


This is a listing of the shaping policies that have been created and their definitions.

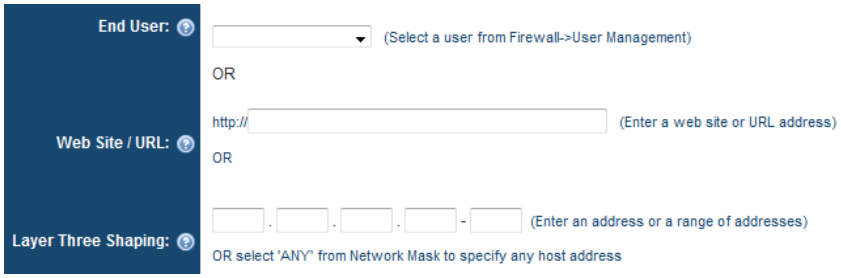
Add Policy (Policy-Based Shaping)

Create a new policy.

AppShaping > EdgeXOS Routing > Policy-Based Shaping > Add Policy



Select a shaping group or define one by clicking on **Bandwidth Groups**.


End User:
(Select a user from Firewall->User Management)
OR
Web Site / URL:
http://
(Enter a web site or URL address)
OR
Layer Three Shaping:
(Enter an address or a range of addresses)
OR select 'ANY' from Network Mask to specify any host address

End User: Shape end-user traffic by IP address, port, or signature.

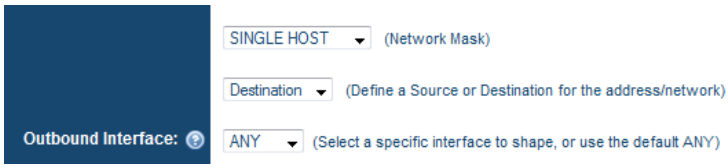
OR

Web Site/URL: Enter the web site URL that you wish to rate-shape using the selected bandwidth group above.

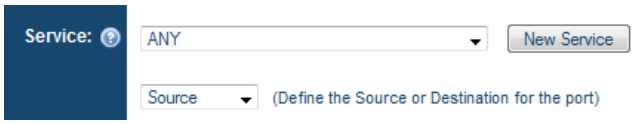
OR

Layer Three Shaping: Enter the Source Address of the traffic to be shaped and/or the subnet mask, then enter the TCP/UDP port to be shaped. If ANY is selected in the network mask field, then any address will match and only the port will be used to shape the traffic.

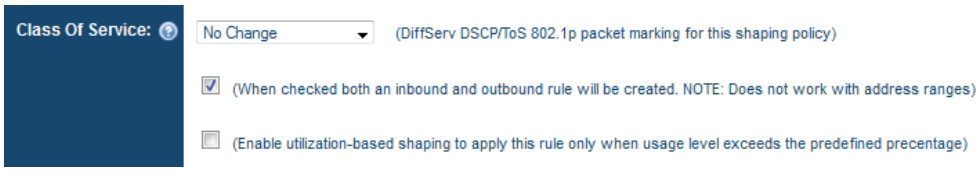
AppShaping > EdgeXOS Routing > Policy-Based Shaping > Add Policy



Use this to select the interface to which traffic will be shaped. Shaping can only effect outbound traffic, i.e. traffic which is leaving an interface, thus to shape inbound traffic, you must use the LAN interface, or ANY and to effect outbound traffic you must slect a WAN interface or ANY.



Select one of the predefined services, or create a service by selecting a protocol and entering a port address.


Class Of Service:
No Change
(DiffServ DSCP/ToS 802.1p packet marking for this shaping policy)
(When checked both an inbound and outbound rule will be created. NOTE: Does not work with address ranges)
(Enable utilization-based shaping to apply this rule only when usage level exceeds the predefined precentage)

Select the level of service for this policy. This will affect the ToS (Type of Service) bit for the matched packets.

Reset: Restores previous settings.

Add/Update: Adds a new policy or updates an existing policy with new settings.

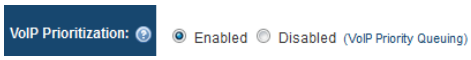
View Policies>>: Returns you to the Shaping Definition List page.

Apply Policies: Forces the application of any newly created policies.

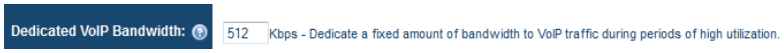
VoIP Shaping & QoS

The EdgeXOS platform includes built-in VoIP QoS shaping to ensure that voice traffic always has priority over other traffic. By default all voice traffic is sent over the primary (WAN1) interface at the highest priority. This can be changed based on the administrators preferences.

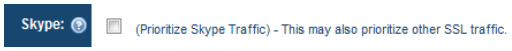
AppShaping > EdgeXOS Routing > VoIP Shaping & QoS



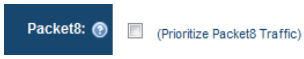
VoIP Prioritization: This feature provides the ability to instantly optimize most SIP-based VoIP traffic. VoIP traffic is given priority queuing and bandwidth is partitioned to ensure high-quality VoIP connectivity.


Dedicated VoIP Bandwidth:
512
Kbps - Dedicate a fixed amount of bandwidth to VoIP traffic during periods of high utilization.

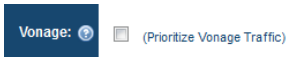
Dedicated VoIP Bandwidth: Use these paramters to determine how much bandwidth will be set aside for VoIP traffic.



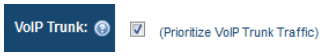
Skype: Use these paramters to determine how much bandwidth will be set aside for VoIP traffic.



Packet8: Use these paramters to determine how much bandwidth will be set aside for VoIP traffic.

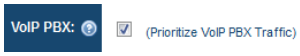


Vonage: Use these paramters to determine how much bandwidth will be set aside for VoIP traffic.

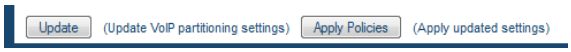


VoIP Trunk: Use these paramters to determine how much bandwidth will be set aside for VoIP traffic.

AppShaping > EdgeXOS Routing > VoIP Shaping & QoS



VoIP PBX: Use these paramters to determine how much bandwidth will be set aside for VoIP traffic.



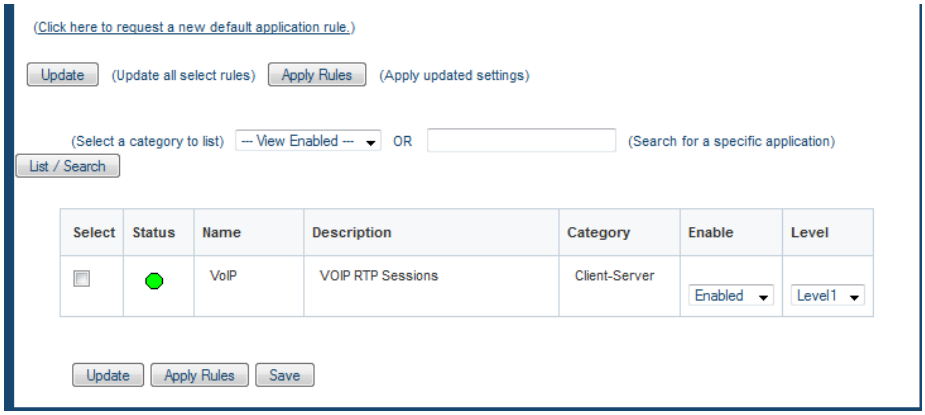
Update: Updates VoIP partitioning settings.

Apply Policies: Immediately applies the updated settings.

Application Shaping

Create specific shaping policies for mission critical applications like HTTP, SSL, and VoIP.

AppShaping > EdgeXOS Routing > Application Shaping

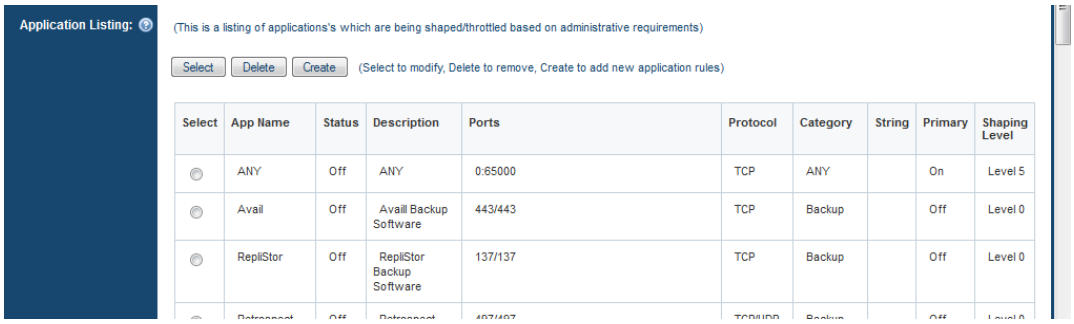


???: ???.

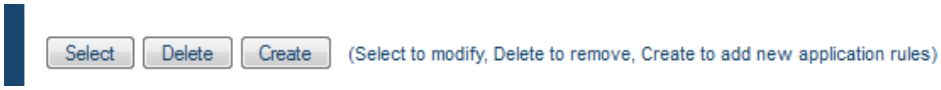
Application Mgmt

Assign a priority level for an application.

AppShaping > EdgeXOS Routing > Application Mgmt



Application Listing: Use this menu to create and manage the applications (and their definitions) which you wish to prioritize. Each application can be assigned to a group/category and then set to one of five different priority levels.



Select: Select an application rule.

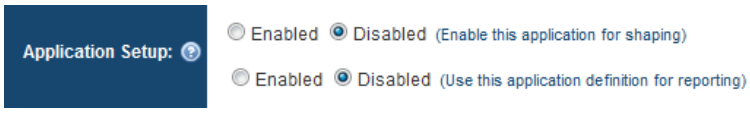
Delete: Delete an application rules.

Create: Create an application rule.

Create Application Rule

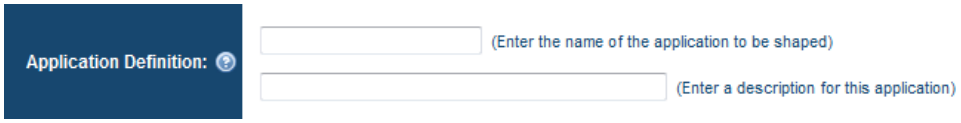
Define a new application.

AppShaping > EdgeXOS Routing > Application Mgmt > Create Application Rule

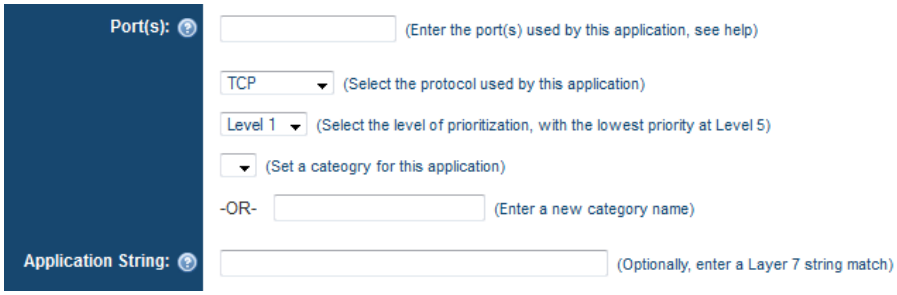


Application Setup: Define a custom application to be managed.

AppShaping > EdgeXOS Routing > Application Mgmt > Create Application Rule



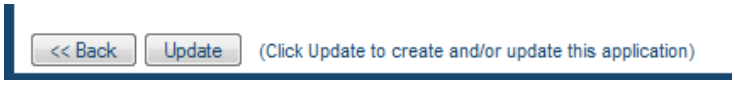
Application Definition: Define a name and description for this application.


Port(s):
(Enter the port(s) used by this application, see help)
TCP
(Select the protocol used by this application)
Level 1
(Select the level of prioritization, with the lowest priority at Level 5)
(Set a cateogry for this application)
-OR-
(Enter a new category name)
Application String:
(Optionally, enter a Layer 7 string match)

Ports: Define the TCP/UDP ports, the level of prioritization and select a category to assign to this application.

OR

Application String: Optionally a string value may be assigned in order to attempt to identify the application, typically not recommended as it can capture many applications.



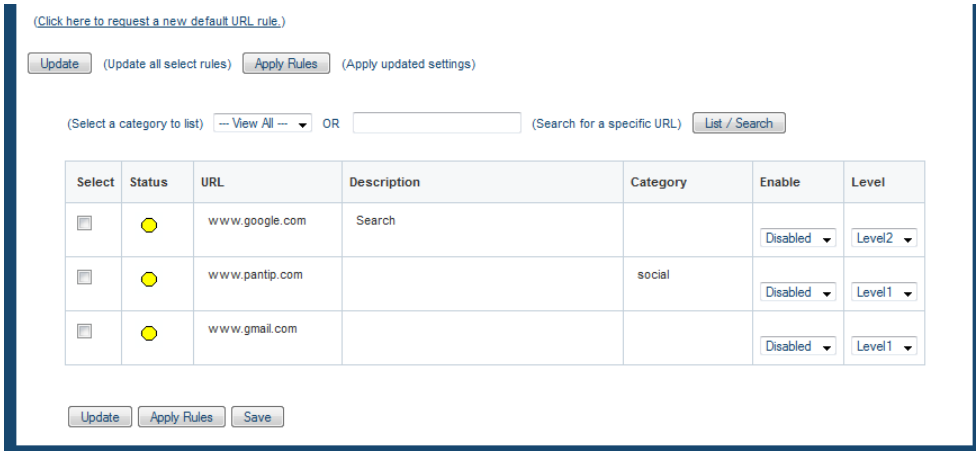
<<Back: Return to the Application Management page.

Update: Update an application rule.

URL Shaping

Create shaping policies based on the URL and/or domain name for an application.

AppShaping > EdgeXOS Routing > URL Shaping

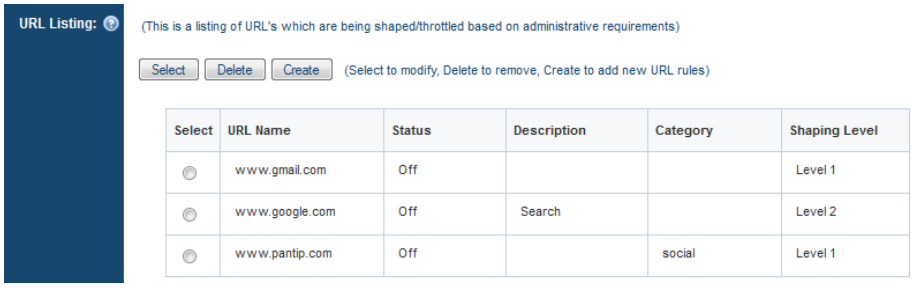


Initially provides a list of existing URLs and their status.

URL Mgmt

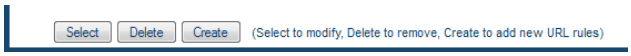
Assign a priority level for a previously defined URL.

AppShaping > EdgeXOS Routing > URL Mgmt



URL Listing: Use this menu to create and manage the URLs which you wish to prioritize. Each URL can be assigned to a group/category and then set to one of five different priority levels.

AppShaping > EdgeXOS Routing > URL Mgmt



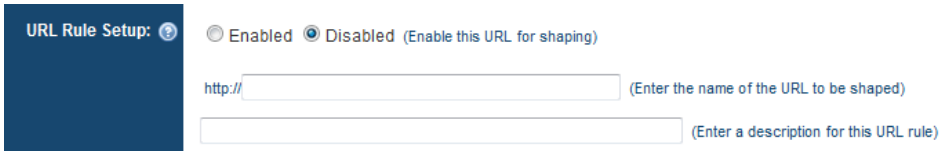
Select: Select a URL rule.

Delete: Delete a URL rule.

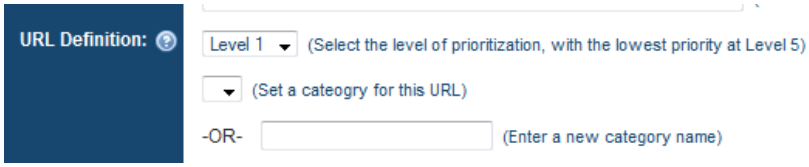
Create: Update a URL rule.

Create URL Rule

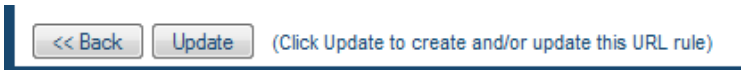
AppShaping > EdgeXOS Routing > URL Mgmt > Create URL Rule



URL Rule Setup: Define a custom application to be managed.


URL Definition:
Level 1
(Select the level of prioritization, with the lowest priority at Level 5)
(Set a cateogry for this URL)
-OR-
(Enter a new category name)

URL Definition: Define a name and description for this application.

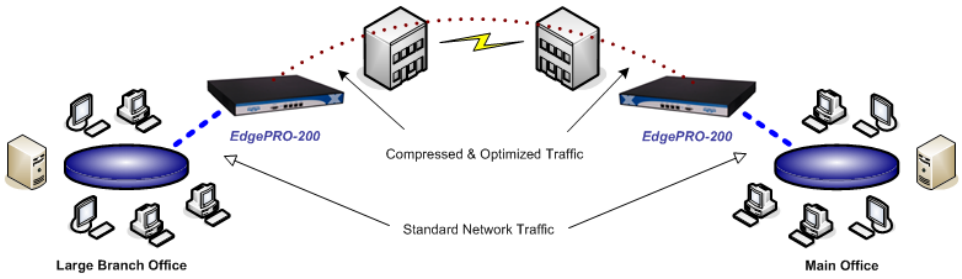


<<Back: Return to the URL Management page.

Update: Update a URL rule.

Site2Site Configuration

Use this guide as a step-by-step manual for configuring the EdgeXOS platform for site-to-site connectivity between two EdgeXOS appliances. The examples provided herein are designed as a template which can translate to your organizations network environment. The three primary configuration steps are 1) Primary hub side tunnel configuration, 2) Primary client side tunnel configuration, and 3) Secondary hub and client side tunnel configuration (for failover and/or load balancing).



Site2Site Overview

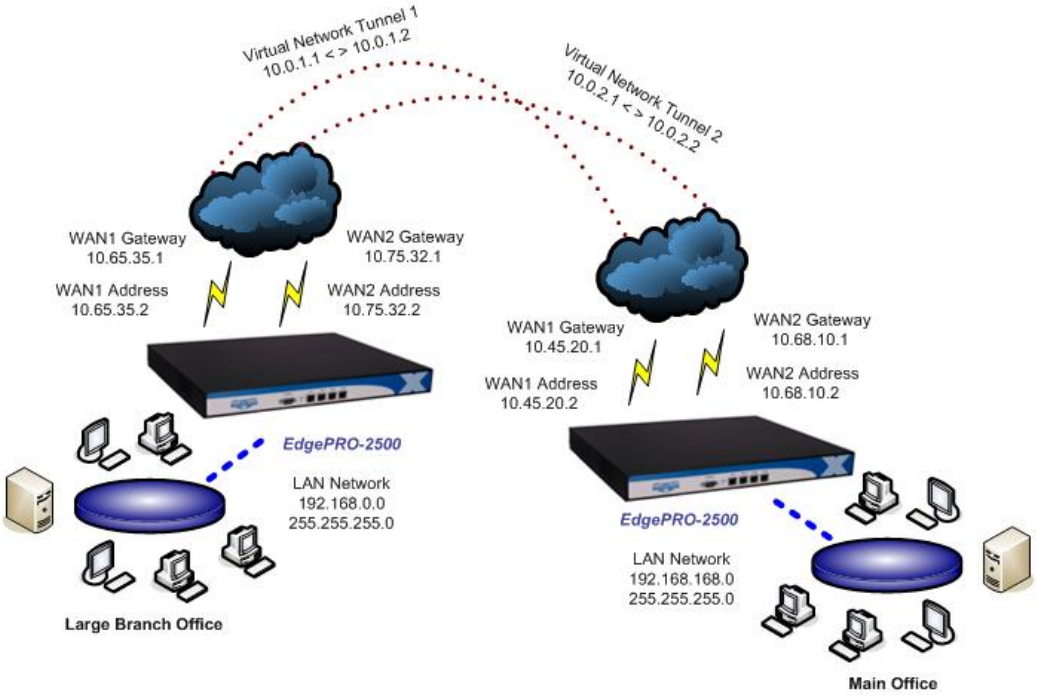
Our Site2Site technology is designed to provide improved connectivity between two or more offices where at least one office has two or more WAN connections. One of the core capabilities of the Site2Site technology is the ability to quickly failover connectivity between two sites when the primary connection is a point-to-point or MPLS connection. In these situations the EdgeXOS platform can provide instant and immediate failover for remote sites using an inexpensive broadband Internet connection via one or more secure encrypted tunnel(s).

Site2Site Example Configuration

This is the **Site2Site** VPN solution with built-in data compression technology. The XOS site to site tunnel can provide instant tunnel failover for branch office/remote office 24x7 connectivity as well as tunnel load balancing between two or more sites for faster downloads and quicker response times for critical applications.

Example Network

This example network is provided as a template which can be used to determine how to best configure your Edge appliance. In the example network environment, each Edge appliance is connected to two WAN interfaces. The WAN interfaces are statically routed in this case, but the method of WAN connection does not matter when configuring the tunnels. The only requirement is that the interfaces being configured are active.



Network Overview

This example network shows two Edge devices connected via two WAN links at each site. The goal is to create two optimization tunnels between the sites and bind them for increase speed via tunnel load balancing with the ability to automatically failover in the event of a WAN outage.

The primary tunnel will be called m2b_tun1 (b2m_tun1), and the secondary tunnel will be called m2b_tun2 (b2m_tun2). The secondary tunnel will be bound to the primary tunnel.

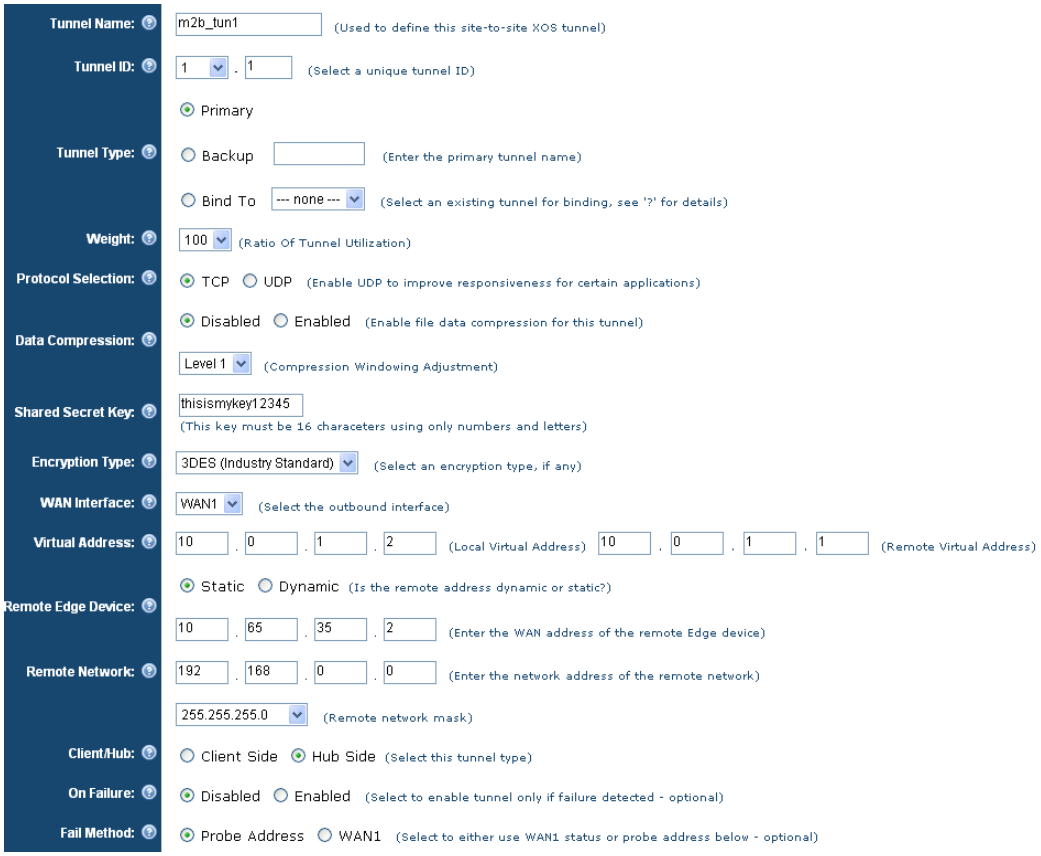
Site2Site Step-By-Step

The following pages show a step-by-step example of how to configure the Edge router based on the network environment in the example scenario.

The following screen will be displayed whenever changes are made to the tunnel rules.

Step One

The following screen demonstrates how TUNNEL 1 on the HUB device is configured.


Tunnel Name: m2b_tun1 (Used to define this site-to-site XOS tunnel)
Tunnel ID: 1 . 1 (Select a unique tunnel ID)
Tunnel Type: Primary
Backup (Enter the primary tunnel name)
Bind To --- none --- (Select an existing tunnel for binding, see '?' for details)
Weight: 100 (Ratio Of Tunnel Utilization)
Protocol Selection: TCP UDP (Enable UDP to improve responsiveness for certain applications)
Data Compression: Disabled Enabled (Enable file data compression for this tunnel)
Level 1 (Compression Windowing Adjustment)
Shared Secret Key: thisismykey12345
(This key must be 16 characeters using only numbers and letters)
Encryption Type: 3DES (Industry Standard) (Select an encryption type, if any)
WAN Interface: WAN1 (Select the outbound interface)
Virtual Address: 10 . 0 . 1 . 2 (Local Virtual Address) 10 . 0 . 1 . 1 (Remote Virtual Address)
Remote Edge Device: Static Dynamic (Is the remote address dynamic or static?)
10 . 65 . 35 . 2 (Enter the WAN address of the remote Edge device)
Remote Network: 192 . 168 . 0 . 0 (Enter the network address of the remote network)
255.255.255.0 (Remote network mask)
Client/Hub: Client Side Hub Side (Select this tunnel type)
On Failure: Disabled Enabled (Select to enable tunnel only if failure detected - optional)
Fail Method: Probe Address WAN1 (Select to either use WAN1 status or probe address below - optional)

Step Two

This screen demonstrates how TUNNEL 1 on the CLIENT device is configured.

Tunnel Name: m2b_tun1 (Used to define this site-to-site XOS tunnel)
Tunnel ID: 1 . 1 (Select a unique tunnel ID)
Tunnel Type: Primary
Backup (Enter the primary tunnel name)
Bind To --- none --- (Select an existing tunnel for binding, see '?' for details)
Weight: 100 (Ratio Of Tunnel Utilization)
Protocol Selection: TCP UDP (Enable UDP to improve responsiveness for certain applications)
Data Compression: Disabled Enabled (Enable file data compression for this tunnel)
Level 1 (Compression Windowing Adjustment)
Shared Secret Key: thisismykey12345
(This key must be 16 characeters using only numbers and letters)
Encryption Type: 3DES (Industry Standard) (Select an encryption type, if any)
WAN Interface: WAN1 (Select the outbound interface)
Virtual Address: 10 . 0 . 1 . 1 (Local Virtual Address) 10 . 0 . 1 . 2 (Remote Virtual Address)
Remote Edge Device: Static Dynamic (Is the remote address dynamic or static?)
10 . 45 . 20 . 2 (Enter the WAN address of the remote Edge device)
Remote Network: 192 . 168 . 168 . 0 (Enter the network address of the remote network)
255.255.255.0 (Remote network mask)
Client/Hub: Client Side Hub Side (Select this tunnel type)
On Failure: Disabled Enabled (Select to enable tunnel only if failure detected - optional)
Fail Method: Probe Address WAN1 (Select to either use WAN1 status or probe address below - optional)

Step Three

The following screen demonstrates how TUNNEL 2 on the HUB device is configured.

Tunnel Name: m2b_tun2 (Used to define this site-to-site XOS tunnel)
Tunnel ID: 2 . 2 (Select a unique tunnel ID)
Tunnel Type: Primary
Backup (Enter the primary tunnel name)
Bind To m2b_tun2 (Select an existing tunnel for binding, see '?' for details)
Weight: 100 (Ratio Of Tunnel Utilization)
Protocol Selection: TCP UDP (Enable UDP to improve responsiveness for certain applications)
Data Compression: Disabled Enabled (Enable file data compression for this tunnel)
Level 1 (Compression Windowing Adjustment)
Shared Secret Key: thisismykey12345
(This key must be 16 characeters using only numbers and letters)
Encryption Type: 3DES (Industry Standard) (Select an encryption type, if any)
WAN Interface: WAN2 (Select the outbound interface)
Virtual Address: 10 . 0 . 2 . 2 (Local Virtual Address) 10 . 0 . 2 . 1 (Remote Virtual Address)
Remote Edge Device: Static Dynamic (Is the remote address dynamic or static?)
10 . 75 . 32 . 2 (Enter the WAN address of the remote Edge device)
Remote Network: 192 . 168 . 0 . 0 (Enter the network address of the remote network)
255.255.255.0 (Remote network mask)
Client/Hub: Client Side Hub Side (Select this tunnel type)
On Failure: Disabled Enabled (Select to enable tunnel only if failure detected - optional)
Fail Method: Probe Address WAN1 (Select to either use WAN1 status or probe address below - optional)

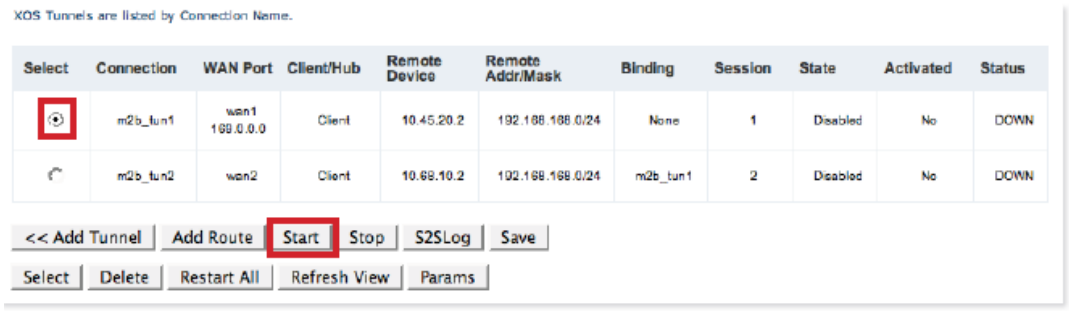
Step Four

This screen demonstrates how TUNNEL 2 on the CLIENT device is configured.

Tunnel Name: m2b_tun2 (Used to define this site-to-site XOS tunnel)
Tunnel ID: 2 . 2 (Select a unique tunnel ID)
Tunnel Type: Primary
Backup (Enter the primary tunnel name)
Bind To m2b_tun2 (Select an existing tunnel for binding, see '?' for details)
Weight: 100 (Ratio Of Tunnel Utilization)
Protocol Selection: TCP UDP (Enable UDP to improve responsiveness for certain applications)
Data Compression: Disabled Enabled (Enable file data compression for this tunnel)
Level 1 (Compression Windowing Adjustment)
Shared Secret Key: thisismykey12345
(This key must be 16 characeters using only numbers and letters)
Encryption Type: 3DES (Industry Standard) (Select an encryption type, if any)
WAN Interface: WAN2 (Select the outbound interface)
Virtual Address: 10 . 0 . 2 . 1 (Local Virtual Address) 10 . 0 . 2 . 2 (Remote Virtual Address)
Remote Edge Device: Static Dynamic (Is the remote address dynamic or static?)
10 . 68 . 10 . 2 (Enter the WAN address of the remote Edge device)
Remote Network: 192 . 168 . 168 . 0 (Enter the network address of the remote network)
255.255.255.0 (Remote network mask)
Client/Hub: Client Side Hub Side (Select this tunnel type)
On Failure: Disabled Enabled (Select to enable tunnel only if failure detected - optional)
Fail Method: Probe Address WAN1 (Select to either use WAN1 status or probe address below - optional)

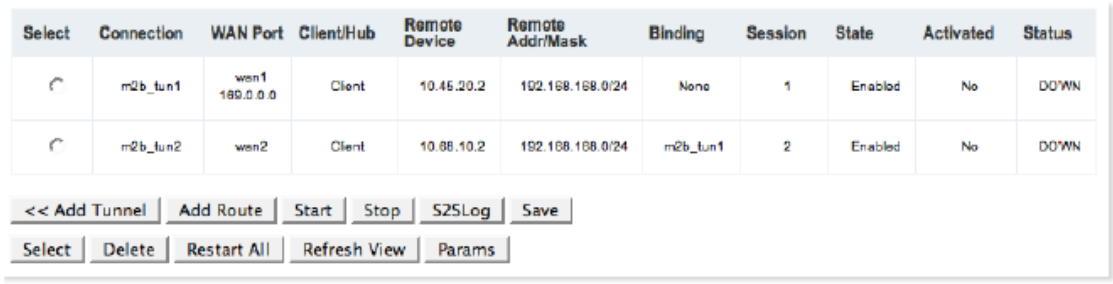
Step Five

Once the tunnels have been created they must be ENABLED. This is done by selecting a tunnel and clicking the "Start" button. This will change the State of the tunnel to ENABLED and the tunnel will attempt to make a connection to the remote Edge device.



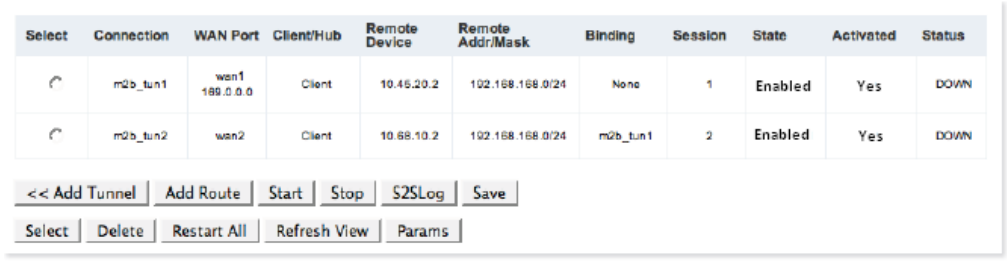
The following screen is displayed during the starting or stopping of a tunnel.

Both tunnels should be ENABLED to enable tunnel binding.



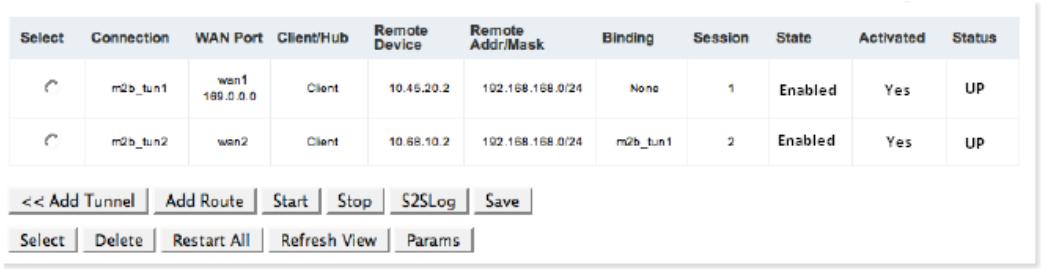
Step Six

The client tunnels must also be started as the hub tunnels were in order to bring the tunnels to an UP and activated mode.



Step Seven

This screen shows the tunnels UP and activated. Both tunnels are now in a load balanced state able to pass traffic between the two sites with full optimization, data compression, error checking, and redundancy.



Select	Connection	WAN Port	Client/Hub	Remote Device	Remote Addr/Mask	Binding	Session	State	Activated	Status
○	m2b_tun1	wan1 169.0.0.0	Client	10.45.20.2	192.168.168.0/24	None	1	Enabled	Yes	UP
○	m2b_tun2	wan2	Client	10.68.10.2	192.168.168.0/24	m2b_tun1	2	Enabled	Yes	UP

Activation / Status Definitions

The "Status" column is used to provide information regarding the availability of the tunnel. If the tunnel is in a working state, the "Status" column will show as UP. If the tunnel is not in a working state, due to either a WAN failure, route failure, disabled or stopped tunnel the "Status" column will show the tunnel as DOWN.

The "Activated" column is used to determine whether the tunnel is being actively routed, meaning whether network traffic is actually being routed through that particular tunnel. If the "Activated" column equals -Yes- than traffic is being routed over this tunnel. If the "Activated" column equals -No- than traffic is not being routed over this tunnel.

Activated	Status
Yes	UP
Yes	UP

This state shows both tunnels UP in load balanced mode.

Activated	Status
Yes	UP
No	DOWN

This state shows the primary tunnel UP and the secondary tunnel DOWN, most likely from a WAN failure or if the tunnel was disabled.

Activated	Status
Yes	UP
Yes	DOWN

This state show the primary tunnel UP and routing traffic. The secondary tunnel is also UP (meaning available) however it is not routing traffic. This is most likely because the tunnel is in Backup mode.

Site2Site WAN Optimization

XRoads Networks offers a new method to deliver increased throughput between sites. Most WAN Optimization technologies utilize caching and various types of data compression to improve speeds.

Existing WAN Optimization Problems

The primary problems with existing WAN optimization techniques is that they are expensive to scale, and are lacking in their ability to optimize small packet bi-directional traffic (applications like Citrix, RDP, VoIP, etc). Most WAN optimization devices rely on two techniques, data caching, which only works for short-term retransmissions, and TCP window scaling, which is usually slow to adjust to small packet traffic.

Site2Site WAN Optimization Solution

XRoads Networks has chosen a "different path" in regards to WAN optimization. Instead of simply caching traffic and trying to guess what is in a packet the Edge appliance actually increases the amount of bandwidth available using inexpensive broadband links.

The advantages to using multiple broadband links are numerous, and the cost is still less than most scalable WAN optimization solutions. Most WAN optimization solutions become oversaturated within several years and become obsolete. The Edge continues its ROI beyond most WAN optimization appliances by allowing the connection of additional inexpensive broadband connections in order to easily increase throughput as needed, a step-up approach which works well with most IT budgets. The Edge's scalability makes this process easy and affordable.

The most unique aspect of the Site2Site tunneling system developed by XRoads Networks is that unlike any other WAN optimization solution, the Site2Site tunnels are 100% network outage resistant. By connecting multiple WAN links on each end of the tunnel, the Edge can achieve over 99.9999% uptime between sites. No other independent WAN optimization solution can make this claim.

Site2Site Data Compression Statistics

Based on tunnel testing using un-compressed text files, the Edge platform was able to achieve a 5:1 increase on download speed and a 3:1 increase in overall download time. Example: A normal download over the Internet took 35 seconds and max'd out at 90Kbps, the same download over our XOS tunnel took 8-9 seconds and max'd out at 450Kbps.

If you multiply that across the multi-WAN capability of our Edge platform you get an overall network throughput increase of up to 30:1 (or 5:1 x 6 load balanced WAN ports). Based on real-world tests XRoads Networks has found a max increase in network throughput of over 2100% for un-compressed data files.

XOS Tunnels List

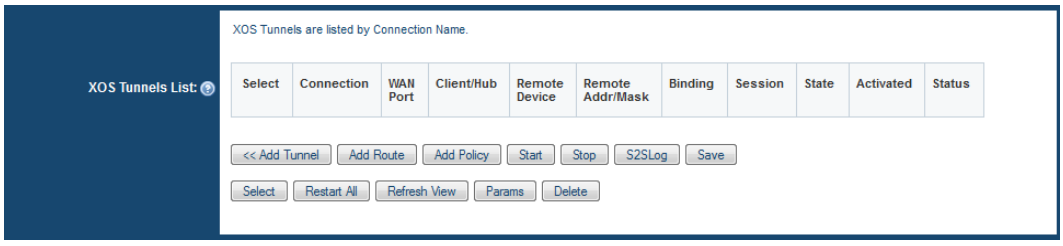
This is a listing of all currently configured WAN Optimization tunnels.

For information on adding an XOS tunnel, see Add Tunnel (XOS).

For information on adding an XOS route, see Add Route (XOS).

For information on adding an XOS policy, see Add Policy (XOS).

For information on the Site2Site log, see S2Slog.



Add Tunnel (XOS)

To setup a tunnel between two EdgeXOS appliances, select the Add Tunnel button and enter the information as outlined below. For more information, see the example provided above and/or the Site2Site How To Guide.

Site2Site > Add Tunnel

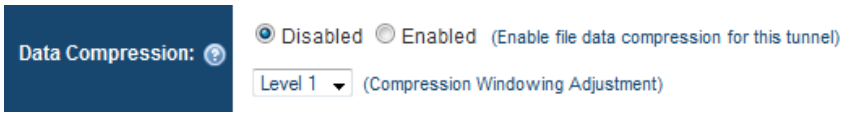
Tunnel Name: Enter the WAN Optimization connection name that will be used for this tunnel, make sure that it is difference from all other connection names.

Tunnel ID: Enter the tunnel ID which will be assigned to this tunnel. The tunnel ID is composed of the session number (obtained from the drop-down), and a unique tunnel number which must match up to tunnel number defined at the opposite end of the connection.

Tunnel Type: If this tunnel will be bound to another tunnel for session load balancing between sites, enter select the primary tunnel to associate with this tunnel. Do not use a binding for the PRIMARY tunnel, only secondary tunnels.

Weight: Use this selection to determine how sessions across two or more tunnels should be balanced. Generally the ratios should be seen as percentages with the total weight of all bonded tunnels divided by an individual tunnel weight providing for the actual perference of each individual tunnel. Example: If two tunnels are bound and one is set for 80 and the other for 20, then 80 percent of the traffic will be routed out the first tunnel.

Site2Site > Add Tunnel



Data Compression: Use this selection to determine whether to implement data compression. Compression is only useful if most of the tunnel traffic is NOT pre-compressed, this typically means text files, otherwise it is recommended to not use compression.

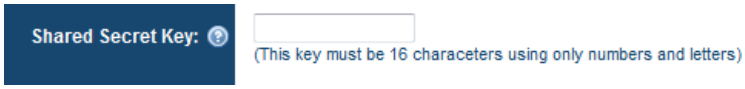
If a majority of the data going through the tunnel is non-compressed, i.e. plain text or large database transfers then data compression could be used to increase the transfer rates across the tunnel(s). Data compression is ONLY useful if the data has not already been compressed as the compression aspect does add some latency and if the data is already compressed it actually increases transit times.

COMPRESSION SPECIFICATIONS: We have completed a number of site-to-site tests between multiple offices. Based on this testing we have confirmed the following compression ratios.

The EdgeXOS platform can achieve a 5:1 increase on download speed and a 3:1 increase in overall download time for non-compressed files. Example: A normal download over the Internet took 35 seconds and max'd out at 90Kbps, the same download over our Site2Site tunnel with compression enabled took 8-9 seconds and max'd out at 450Kbps.

However files that are PRE-compressed, meaning that it was zipped or compressed by another application prior to being downloaded, it will almost always take the same amount of time to download, i.e. no increase in speed or throughput. In fact, under some conditions it may take a bit longer due to the tunnels added overhead.

Tunnel compression is not recommended for use with database applications, Windows remote file access, or real-time streaming applications as it does not provide an increase in speed for those applications.



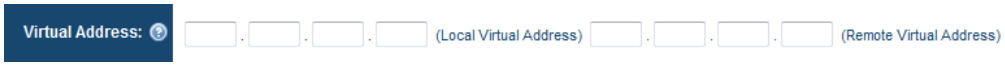
Shared Secret Key: Enter a shared secret key for this tunnel, each side MUST have the exact same key and the key MUST be 16 characters long.

Site2Site > Add Tunnel

Encryption Type: Select an encryption method (if any) to use to ensure secure connectivity across the WAN Optimization tunnel. Keep in mind that any encryption performed on the tunnel will create additional latency.

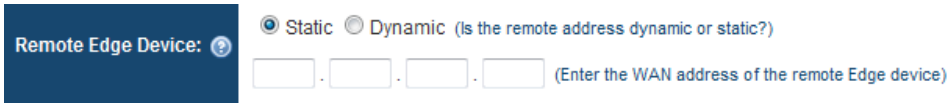
Built-in to each Site2Site tunnel is the ability to encapsulate data using a highly secure encryption algorithm called 3DES. 3DES encryption has long been a standard in the industry and is widely used by the government and banking sector. When setting up a tunnel which will traverse the Internet it is a good idea to enable 3DES encryption in order to provide for some level of protection for the site-to-site data. No encryption is required for tunnels established over a private point-to-point or MPLS connection.

WAN Interface: Select the WAN interface which this tunnel will use when connecting.

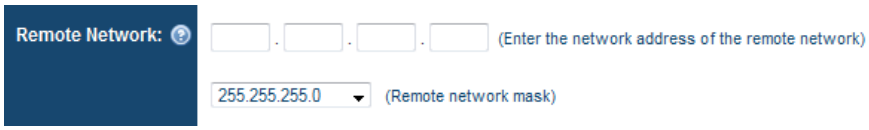


Virtual Address: These IP addresses are used to create a subnet between the WAN Optimization tunnel. This subnet is used for testing the tunnel. In general this is a /30 subnet, a default address pair would be 10.0.0.1 and 10.0.0.2, then use the opposite addressing 10.0.0.2 and 10.0.0.1 at the other end.

Site2Site > Add Tunnel

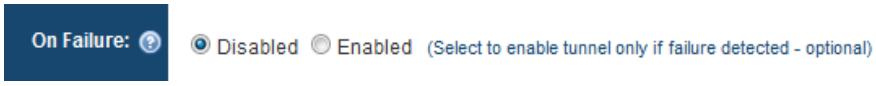

Remote Edge Device:
Static
Dynamic
(Is the remote address dynamic or static?)
(Enter the WAN address of the remote Edge device)

Remote EdgeXOS Device: Select whether the remote address is static or dynamic. Dynamic addresses can only be used by the client, and thus only configured when creating a rule on the hub side of the tunnel. If dynamic leave the address field blank. If static, enter the static IP address the remote devices WAN interface.

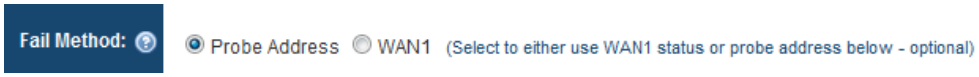


Remote Network: Enter the network address (Example: x.x.x.0) of the remote devices LAN network, then select a matching gateway for the remote LAN network.

Client/Hub: Select the appropriate mode based on function of this side of the tunnel. Regardless, one side MUST be the client and one side MUST be the hub.

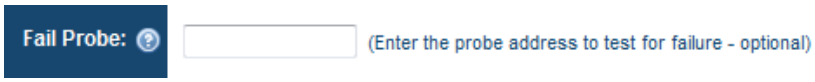


On Failure: Enable this feature on BACKUP tunnels. This will enable the tunnel if either the primary tunnel fails, or if WAN1 fails.



Fail Method: This optional feature is used to turn up a tunnel ONLY if either of the selection options occurs.

Site2Site > Add Tunnel



Fail Probe: Enter the probe address to be used, if the fail method option is selected above.

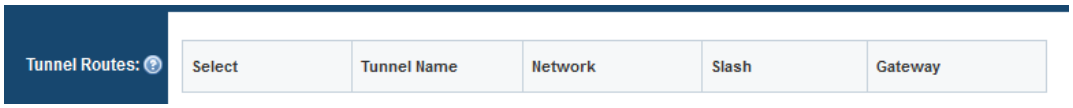
Add/Update: Add a new tunnel or update an existing tunnel.

View Tunnels>>: Return to the XOS Tunnels List page.

Add Route (XOS)

Used to add secondary routes to configured Site2Site tunnels, this is useful if you have multiple networks which need to be routed between two or more sites.

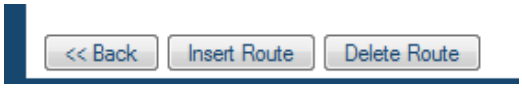
Site2Site > Add Route



Tunnel Routes: Tunnel routing is used to forward additional subnets through a tunnel to a remote network. This is useful when the remote site has a number of other networks that need to be routed at the remote end of the MVLS tunnel.

Insert Route: In order to route additional networks through the tunnel, or to specify that access to another network is available through the tunnel add the route to that network here. Make sure to add a route for each tunnel that is bound or the route could be remove if one of the tunnels loses connectivity. To use this tunnel as a default route add 0.0.0.0/0 as your route.

Site2Site > Add Route



<<Back: Return to the XOS Listings page.

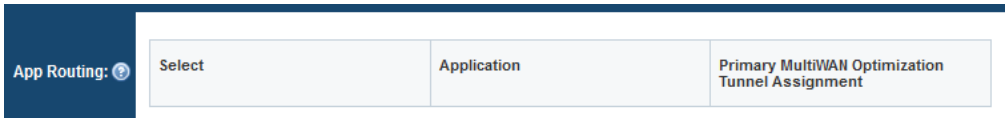
Insert Route: Insert a new tunnel route.

Delete Route: Delete a tunnel route.

Add Policy (XOS)

Use Site2Site policies to redirect specific applications, which are being routed across the Site2Site tunnels via a specific tunnel. Example: If there are two active tunnels between sites and we wish to force all SSL traffic across a specific tunnel, this can be accomplished by adding a policy.

Site2Site > Add Policy



App Routing: Lists the current application policies which have been added.

Insert Policy: Use to route specific application traffic across a specific tunnel.

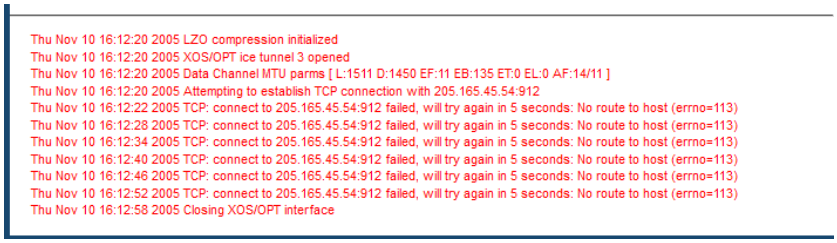
<<Back: Return to the XOS Listings page.

Insert Route: Insert a new policy.

Delete Route: Delete a policy.

S2Slog

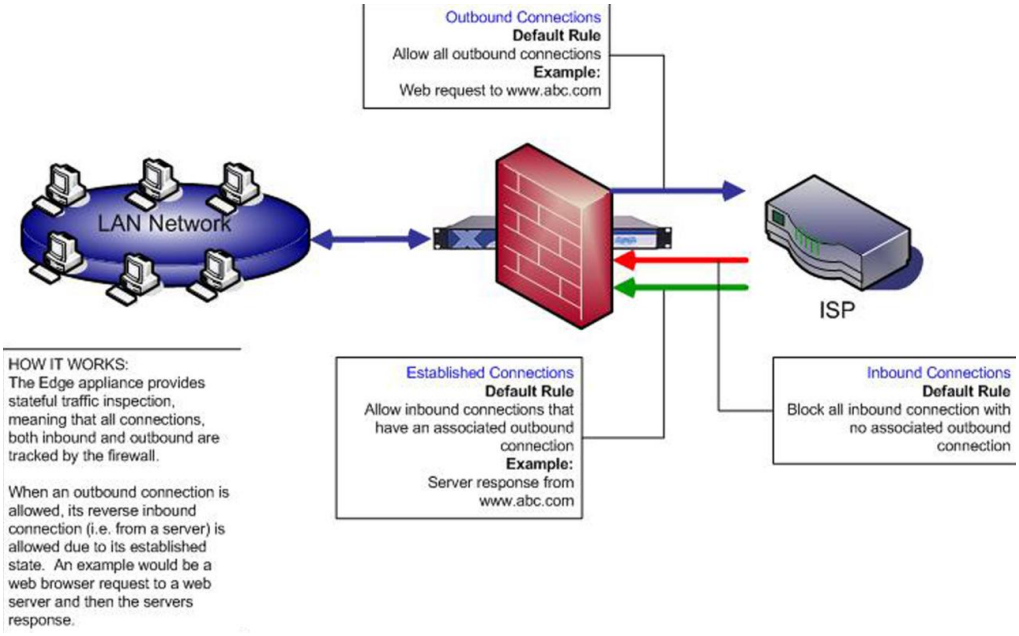
Use the log information to determine where any configuration problems might lie when deploying the Site2Site tunnels.


Thu Nov 10 16:12:20 2005 LZO compression initialized
Thu Nov 10 16:12:20 2005 XOS/OPT ice tunnel 3 opened
Thu Nov 10 16:12:20 2005 Data Channel MTU parms [L:1511 D:1450 EF:11 EB:135 ET:0 EL:0 AF:14/11]
Thu Nov 10 16:12:20 2005 Attempting to establish TCP connection with 205.165.45.54:912
Thu Nov 10 16:12:22 2005 TCP: connect to 205.165.45.54:912 failed, will try again in 5 seconds: No route to host (errno=113)
Thu Nov 10 16:12:28 2005 TCP: connect to 205.165.45.54:912 failed, will try again in 5 seconds: No route to host (errno=113)
Thu Nov 10 16:12:34 2005 TCP: connect to 205.165.45.54:912 failed, will try again in 5 seconds: No route to host (errno=113)
Thu Nov 10 16:12:40 2005 TCP: connect to 205.165.45.54:912 failed, will try again in 5 seconds: No route to host (errno=113)
Thu Nov 10 16:12:46 2005 TCP: connect to 205.165.45.54:912 failed, will try again in 5 seconds: No route to host (errno=113)
Thu Nov 10 16:12:52 2005 TCP: connect to 205.165.45.54:912 failed, will try again in 5 seconds: No route to host (errno=113)
Thu Nov 10 16:12:58 2005 Closing XOS/OPT interface

Security and Firewall Features

The EdgeXOS appliance includes a fully stateful and hardened firewall. Our firewall meets the highest standards in terms of network security and the ability to block unwanted access to the internal network.

The firewall has been certified as being compliant with ICSA standards and has passed multiple tests to become PCI compliant for ecommerce networks.


Outbound Connections
Default Rule
Allow all outbound connections
Example:
Web request to www.abc.com
LAN Network
ISP
HOW IT WORKS:
The Edge appliance provides stateful traffic inspection, meaning that all connections, both inbound and outbound are tracked by the firewall.
When an outbound connection is allowed, its reverse inbound connection (i.e. from a server) is allowed due to its established state. An example would be a web browser request to a web server and then the servers response.
Established Connections
Default Rule
Allow inbound connections that have an associated outbound connection
Example:
Server response from www.abc.com
Inbound Connections
Default Rule
Block all inbound connection with no associated outbound connection

Firewall Overview

The firewall components are designed to provide network administrators with a complete cloud security system, from a layer-7 stateful firewall to built-in web content filtering, and enhanced anti-spyware and anti-virus filtering, to remote access software to allow teleworkers to connect to the local network, the EdgeXOS platform is a complete security solution. The EdgeXOS firewall also includes enterprise class email and anti-spam filtering along with on and offsite backup solutions. The EdgeXOS platform is able to achieve its industry leading

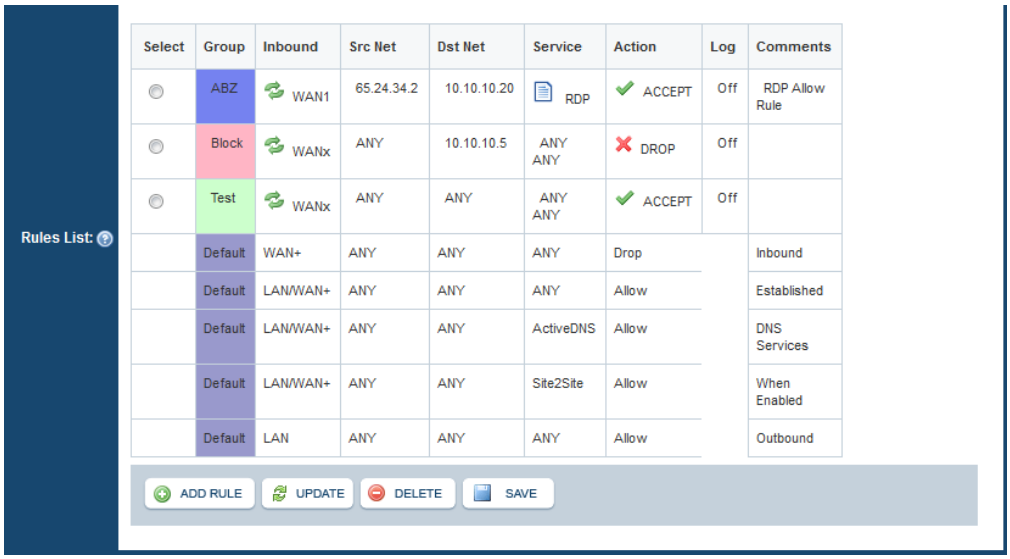
security solution through strategic partnerships with companies like Webroot. These companies provide the databases and filtering capabilities that our solutions utilize to provide our enhanced security offerings.

- L7 Firewall Rules
- L7 Firewall Control
- L7 Firewall User Management
- L7 Firewall DoS / SYN Filtering
- L7 Firewall Global Web Filtering
- Display NAT Rules
- Vector Routing (Outbound)
- One-To-Many NAT (PAT)
- One-To-One NAT (SNAT)
- Remote Access Site2Site Client
- Remote Access PPTP Client
- User/Device Access Control (NAC)

L7 Firewall Rules

Use this menu option to create and configured new rules which the firewall will use to allow and/or deny network traffic, based on IP address, network, application, port/protocol, and/or signature.

Firewall > EdgeXOS Security > L7 Firewall Rules



Rules List: This list contains all of the administratively applied EdgeXOS firewall rules.

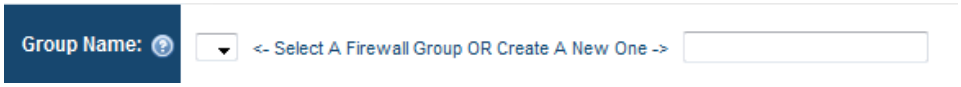
Add Rule

The firewall module is primarily controlled by creating firewall rules which either allow or deny traffic through the EdgeXOS appliance. The firewall rules can be applied to ALL or any individual network interfaces.

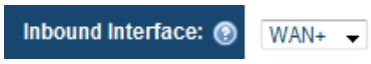
Rules are applied in ALPABETICAL ORDER based on the Group Name. Firewall rules are applied in a first to match method. In other words, the first rule to match the particular type of traffic will apply. If no rule matches, the default rules apply.

NOTE: By default, all outbound access is allowed. By default, all inbound access is denied. Example: All inbound server traffic is denied by default, and all outbound LAN network traffic is allowed by default.

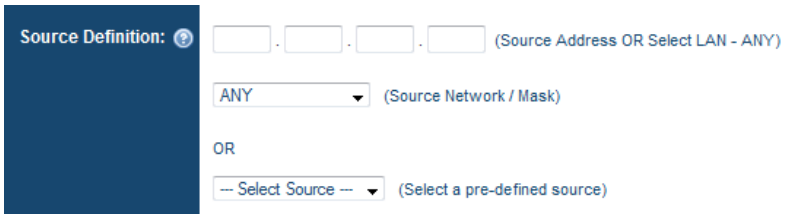
Firewall > L7 Firewall Rules > Add Rule



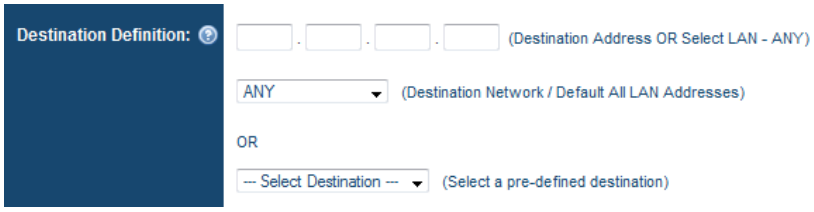
Group Name: Use this section to select or create a group to assign this firewall rule. This makes administration easier and more flexible.



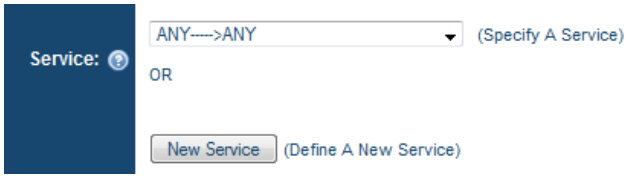
Inbound Interface: Select the interface to which you wish to apply these EdgeXOS firewall rules.



Source Definition: Enter the source network and subnet from which the rule should be applied.

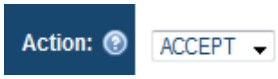


Destination Definition: Enter the destination network and subnet from which the rule should be applied.

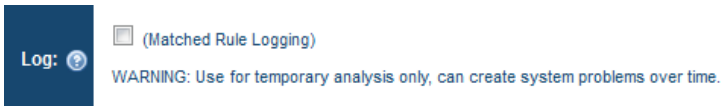


Service: Select one of the predefined services, or create a service by selecting a protocol and entering a port address.

Firewall > L7 Firewall Rules > Add Rule



Action: Select the action to be applied to this EdgeXOS firewall rule.



Log: Select whether to log whenever these rule is matched by the XRoads EdgeXOS firewall.

Color: Select a color to assign to this rule, or leave default for the default colors.

Comments: Enter a description for this rule for easy recognition.

Reset: Reset the rule's settings to their last saved state.

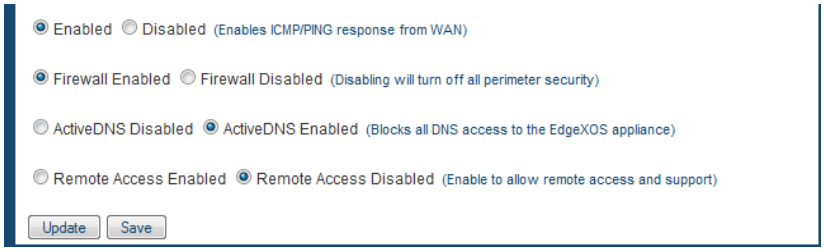
Add/Update: Add or update a firewall rules.

View Rules>>: Return to the main L7 Firewall Rules page.

L7 Firewall Control

Use these options to enable and/or disable various firewall functionality, including the ability to allow remote access by XRoads Networks support department.

Firewall > EdgeXOS Security > L7 Firewall Control


Enabled Disabled (Enables ICMP/PING response from WAN)
Firewall Enabled Firewall Disabled (Disabling will turn off all perimeter security)
ActiveDNS Disabled ActiveDNS Enabled (Blocks all DNS access to the EdgeXOS appliance)
Remote Access Enabled Remote Access Disabled (Enable to allow remote access and support)
Update
Save

Enabled / **Disabled**: Enables ICMP/PING response from WAN

Firewall Enabled / **Firewall Disabled**: Disabling will turn off all perimeter security

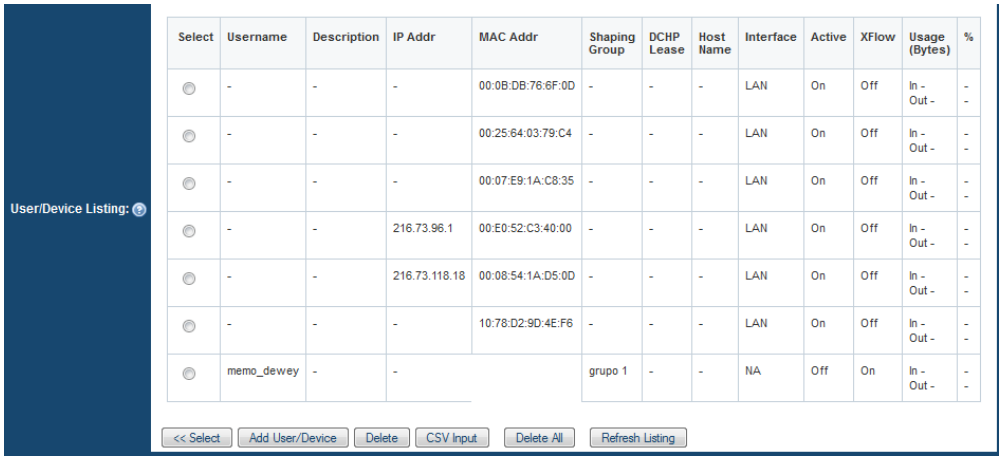
Active DNS Disabled / **Active DNS Enabled**: Blocks all DNS access to the EdgeXOS appliance

Remote Access Enabled / **Remote Access Disabled**: Enable to allow remote access and support

L7 Firewall User Management

This menu option accesses the user management feature of the firewall which allows network administrators to view and label users based on their MAC addresses. User Management is also used to control VPN authentication as well as assign per user bandwidth shaping policies. To add a user or device for L7 firewall management, see Add User/Device.

Firewall > EdgeXOS Security > L7 Firewall User Management



User/Device Listing: This is a listing of all alert emails that have been configured. When an alert occurs, the associated email addressee will be notified.

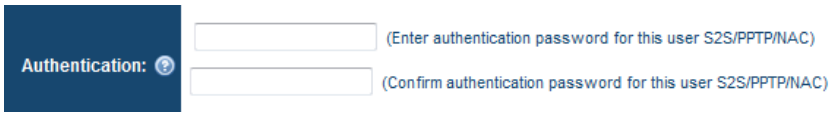
Add User/Device

Use this option to add new devices to the User Management system.

Firewall > L7 Firewall Rules > Add Rule

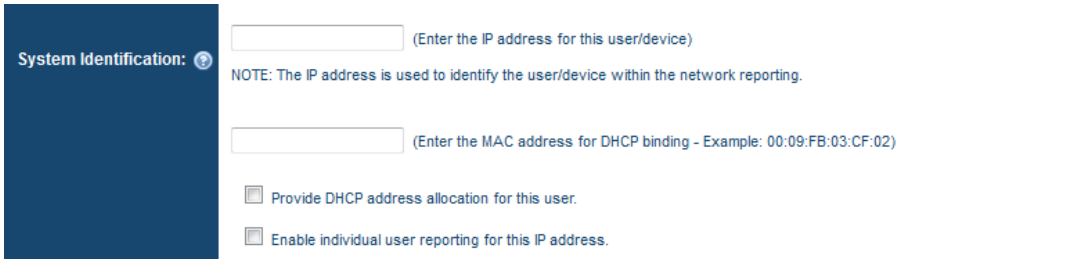
User/Device Information:
(Name for this user/device, i.e. webserver or jsmith)
NOTE: This name is used to identify the user/device within the network reporting.
(Description or comment for this user/device)

User/Device Information: Enter the name of the person who will receive these messages.


Authentication:
(Enter authentication password for this user S2S/PPTP/NAC)
(Confirm authentication password for this user S2S/PPTP/NAC)

Authentication: Use these fields to enter the authentication password to be used when the AUP page authorization is enabled.

Firewall > L7 Firewall Rules > Add Rule


System Identification:
(Enter the IP address for this user/device)
NOTE: The IP address is used to identify the user/device within the network reporting.
(Enter the MAC address for DHCP binding - Example: 00:09:FB:03:CF:02)
Provide DHCP address allocation for this user.
Enable individual user reporting for this IP address.

System Identification: Enter the IP address of the mail server which the XRoads router will use when sending out email. Example: 1.1.1.1.

Bandwidth Enforcement: Select the shaping group that you wish to assign to this user. The shaping group is controlled via the Policy-Based Shaping Module.

Reset: Reset the rule's settings to their last saved state.

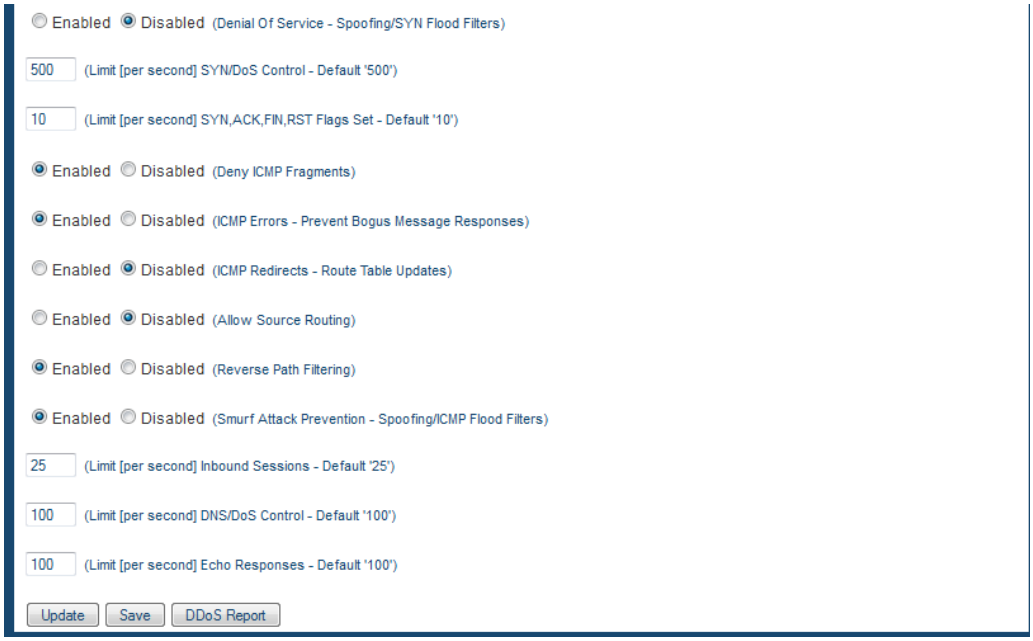
Add/Update: Add or update a firewall rules.

View Users/Devices>>: Return to the main L7 Firewall User Management page.

L7 Firewall DoS / SYN Filtering

DoS (Denial of Service) is a technique used by some hackers to attempt to block connectivity to and from a network. The EdgeXOS appliance provides protection against this type of attack by limiting the number of packets allowed that match certain characteristics generally found in these types of attacks.

Firewall > EdgeXOS Security > L7 DoS/Syn Filtering


Enabled Disabled (Denial Of Service - Spoofing/SYN Flood Filters)
500 (Limit [per second] SYN/DoS Control - Default '500')
10 (Limit [per second] SYN,ACK,FIN,RST Flags Set - Default '10')
Enabled Disabled (Deny ICMP Fragments)
Enabled Disabled (ICMP Errors - Prevent Bogus Message Responses)
Enabled Disabled (ICMP Redirects - Route Table Updates)
Enabled Disabled (Allow Source Routing)
Enabled Disabled (Reverse Path Filtering)
Enabled Disabled (Smurf Attack Prevention - Spoofing/ICMP Flood Filters)
25 (Limit [per second] Inbound Sessions - Default '25')
100 (Limit [per second] DNS/DoS Control - Default '100')
100 (Limit [per second] Echo Responses - Default '100')
Update
Save
DDoS Report

Deny IP Fragments will block IP packets that have been broken up in an attempt to fool the firewall and allow certain types of network connections.

Limits the number of ICMP packets that the firewall will allow.

Limits the number of connection initialization requests that the firewall will allow. This may need to be increased for highly active networks.

Limits the ability for a hacker to scan the firewall for vulnerabilities.

L7 Firewall Global Web Filtering

The Web Filtering module is either a built in option on the appliance purchased or can be added as a licensed feature. The functionality of the Web Filtering is to filter and/or block unwanted content from being accessed

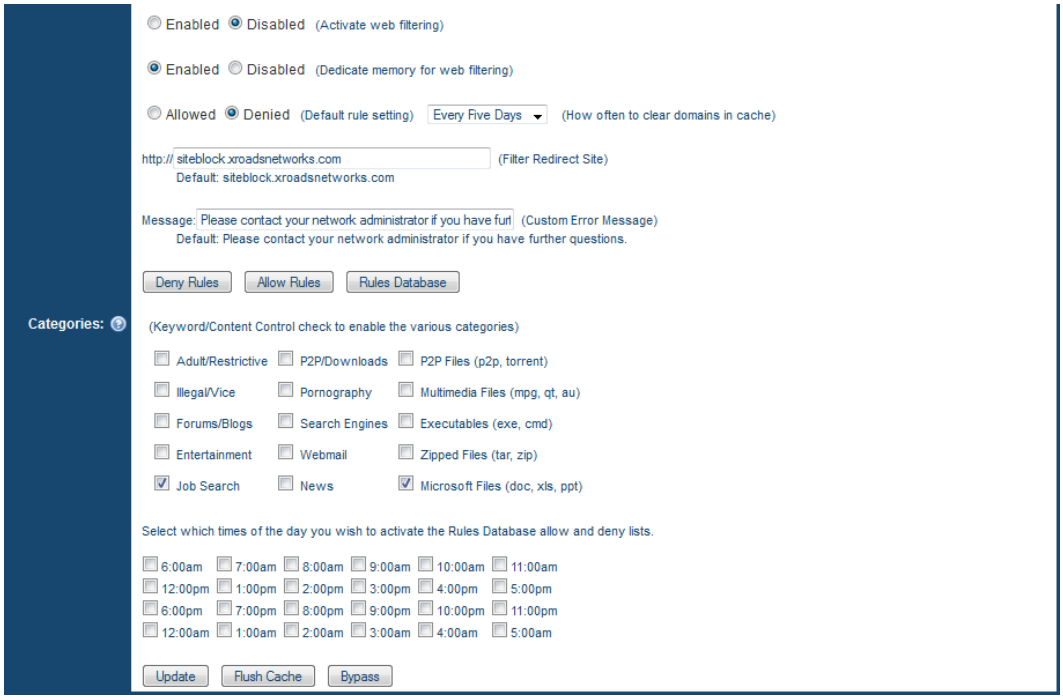
by internal users.

The content which can be blocked includes, P2P, Chat, Instant Messaging, Spyware, File Download services, and various other web sites and multi-media applications.

The filtering works by intercepting DNS and HTTP requests made by internal clients and providing either the appropriate response, or based on the filtering rules, respond with a local host address which essentially blocks the application/web browser from being able to access the selected content.

There are various controls which can be placed on the Web Filtering feature, including the ability to match a device to an actual user name, or setting up a by-pass list.

Firewall > EdgeXOS Security > L7 Firewall Global Web Filtering

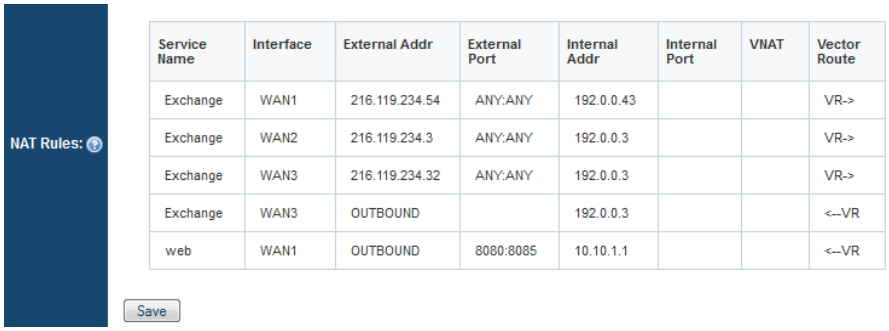

Enabled Disabled (Activate web filtering)
Enabled Disabled (Dedicate memory for web filtering)
Allowed Denied (Default rule setting)
Every Five Days
(How often to clear domains in cache)
http:// siteblock.xroadsnetworks.com (Filter Redirect Site)
Default: siteblock.xroadsnetworks.com
Message: Please contact your network administrator if you have furt (Custom Error Message)
Default: Please contact your network administrator if you have further questions.
Deny Rules
Allow Rules
Rules Database
Categories:
(Keyword/Content Control check to enable the various categories)
Adult/Restrictive
P2P/Downloads
P2P Files (p2p, torrent)
Illegal/Vice
Pornography
Multimedia Files (mpg, qt, au)
Forums/Blogs
Search Engines
Executables (exe, cmd)
Entertainment
Webmail
Zipped Files (tar, zip)
Job Search
News
Microsoft Files (doc, xls, ppt)
Select which times of the day you wish to activate the Rules Database allow and deny lists.
6:00am 7:00am 8:00am 9:00am 10:00am 11:00am
12:00pm 1:00pm 2:00pm 3:00pm 4:00pm 5:00pm
6:00pm 7:00pm 8:00pm 9:00pm 10:00pm 11:00pm
12:00am 1:00am 2:00am 3:00am 4:00am 5:00am
Update
Flush Cache
Bypass

Categories: The following categories are used to filter unauthorized web content. When a category is selected all content which contains these elements will be blocked.

Display NAT Rules

Provides a list of the existing Network Address Translation rules which have been configured within the appliance.

Firewall > EdgeXOS Security > Display NAT Rules

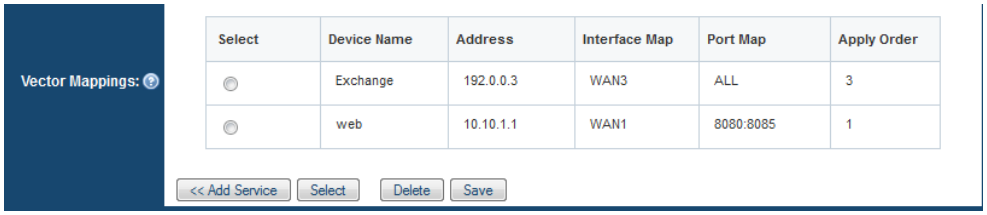


NAT Rules: This list contains all of the administratively applied servers / services. When deleting a selection the two options are Partial Delete and Full Delete, full delete will also remove any secondary addresses added to the WAN interface. This will also cause a momentary loss of network connectivity. To ensure session connectivity only use Partial Delete during normal operating hours and reboot the unit during your next maintanence period to remove any unwanted secondary addresses.

Vector Routing (Outbound)

To add a vector routing rule which ensures that traffic maintains session persistence, see Add Service (Vector Routing).

Firewall > EdgeXOS Security > Vector Routing (Outbound)



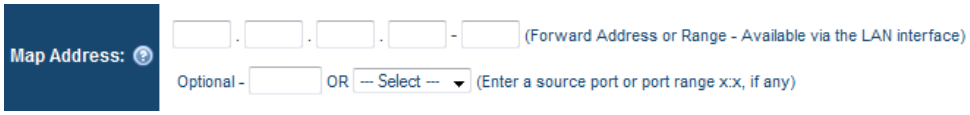
Vector Mapping: This is a listing of the Vector mappings that you have created. This list includes all of the Vector Map entries for quick review.

Add Service (Vector Routing)

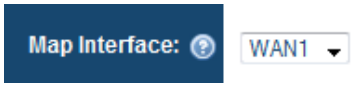
Used to create new Vector Routing rules.

Firewall > Vector Routing (Outbound) > Add Service

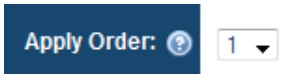
Device Name: Device Name allows you to identify a particular Vector mapping that you have created. It is generally recommended that you use a similar name as the DNS rule you created for this inbound load balancing device.


Map Address:
(Forward Address or Range - Available via the LAN interface)
Optional -
OR
--- Select ---
(Enter a source port or port range x:x, if any)

Map Address: The Map Address is the LAN address (and range of addresses) that are to be assigned to a particular WAN interface. Creating these mappings is required when the unit is in load balance mode AND has inbound traffic via either a proxy config on WAN1 or any advanced NAT mappings. When both of these conditions exist Vector Maps MUST be created. Optionally enter a source address in order to only force response traffic for a particular service and/or application back through the selected WAN interface. Enter VPN as the port number definition in order to specify any IPSec/PPTP VPN connection.



Map Interface: Select the WAN interface that will be used for mapping the internal address to an external gateway. This mapping MUST match your DNS rules in order for load balancing to work correctly.



Apply Order: The APPLY ORDER function is used to allow network administrators control which mappings will be applied and in which order based on the current active state of each WAN link. Only one server mapping can be active at any given time, thus the APPLY ORDER variable allows one to control which mapping will be used and to which WAN link it will be bound.

Firewall > Vector Routing (Outbound) > Add Service

Reset: Reset the rule's settings to their last saved state.

Add/Update: Add or update a firewall rules.

View Services>>: Return to the main Vector Routing (Outbound) page.

One-To-Many NAT (PAT)

Used to create new port address translation rules, see Add Service (One-To-Many NAT).

Firewall > EdgeXOS Security > One-To-Many NAT (PAT)

One-To-Many List: This list contains all of the administratively applied servers / services. When deleting a selection the two options are Partial Delete and Full Delete, full delete will also remove any secondary addresses added to the WAN interface. This will also cause a momentary loss of network connectivity. To ensure session connectivity only use Partial Delete during normal operating hours and reboot the unit during your next maintanence period to remove any unwanted secondary addresses.

Add Service (One-To-Many NAT)

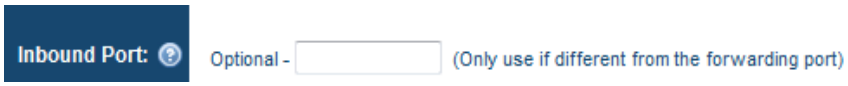
Use this service to create new O2M rules.

Firewall > One-To-Many NAT (PAT) > Add Service

Service Name: Enter a Service Name to identify this NAT rule, the name must be different from any One-To-Many NAT rule you may have entered.
Next, determine how you wish this rule to handle source NATing. Source NATing causes any traffic coming from the defined "Internet Address" to be NATed out the WAN interface using the provided "External Address". This is very useful most of the time, however problems can occur when load balancing multiple connections.

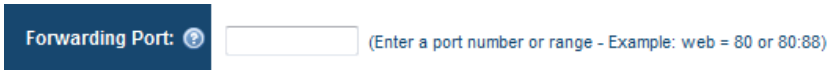
Select the first checkbox when the selected interface is in BACKUP mode, but you still wish to be able to communicate to the defined "Internal Address". Keep in mind that this will not work if you already have a Vector Map defined for this "Internal Address" to use a different WAN port.

Inbound Interface: Select the WAN interface that will be used for inbound NAT translation OR enter a specific address which will be automatically added to the specified WAN interface (a port may also be specified for more granular control). IMPORTANT: Make sure to select the correct interface or the NAT rule will not work. Match the Internet address to the correct Inbound Interface.

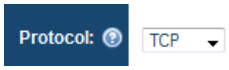


Inbound Port: Select the WAN interface that will be used for inbound NAT translation OR enter a specific address which will be automatically added to the specified WAN interface (a port may also be specified for more granular control). IMPORTANT: Make sure to select the correct interface or the NAT rule will not work. Match the Internet address to the correct Inbound Interface.

Firewall > One-To-Many NAT (PAT) > Add Service

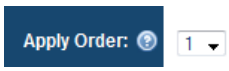


Forwarding Port: Forward Port allows you to identify a port and/or protocol/service for inbound network address translation.



Protocol: Forward Protocol allows you to identify whether the service used TCP or UDP.

Forwarding Address: Forward Address allows you to identify the server to which the protocol/service will be directed. Internet Address - Must be available via the WAN port selected below.



Apply Order: The APPLY ORDER function is used to allow network administrators control which mappings will be applied and in which order based on the current active state of each WAN link. Only one server mapping can be active at any given time, thus the APPLY ORDER variable allows one to control which mapping will be used and to which WAN link it will be bound.

Reset: Reset the rule's settings to their last saved state.

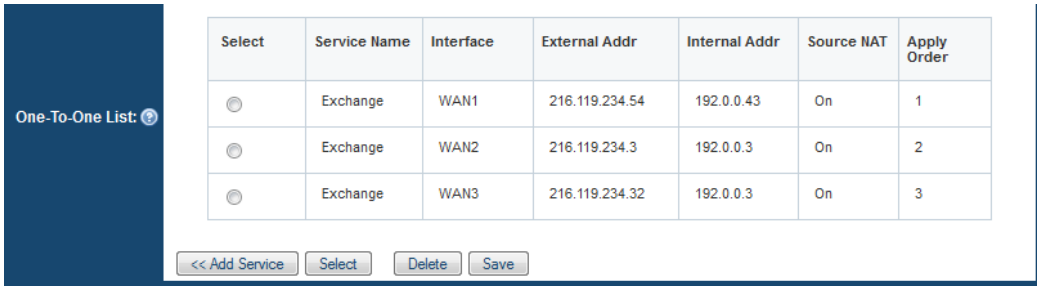
Add/Update: Add or update a firewall rules.

View Services>>: Return to the main One-To-Many NAT page.

One-To-One NAT (SNAT)

Use this service to create new O2O rules.

Firewall > EdgeXOS Security > One-To-One NAT (SNAT)

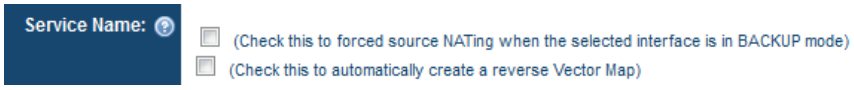


One-To-One List: This list contains all of the administratively applied servers / services. When deleting a selection the two options are Partial Delete and Full Delete, full delete will also remove any secondary addresses added to the WAN interface. This will also cause a momentary loss of network connectivity. To ensure session connectivity only use Partial Delete during normal operating hours and reboot the unit during your next maintanence period to remove any unwanted secondary addresses.

Add Service (One-To-One NAT)

Add a new NAT rule for one-to-one address and port translation.

Firewall > One-To-One NAT (SNAT) > Add Service


Service Name:
(Check this to forced source NATing when the selected interface is in BACKUP mode)
(Check this to automatically create a reverse Vector Map)

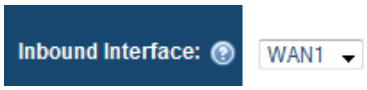
Service Name: Enter a Service Name to identify this NAT rule, the name must be different from any One-To-Many NAT rule you may have entered.

Next, determine how you wish this rule to handle source NATing. Source NATing causes any traffic coming from the defined "Internet Address" to be NATed out the WAN interface using the provided "External Address". This is very useful most of the time, however problems can occur when load balancing multiple connections.

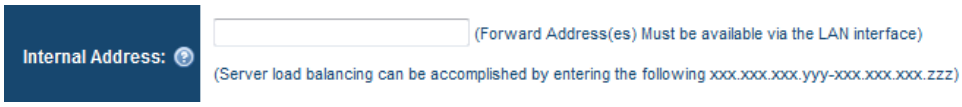
Select the first checkbox when the selected interface is in BACKUP mode, but you still wish to be able to communicate to the defined "Internal Address". Keep in mind that this will not work if you already have a Vector Map defined for this "Internal Address" to use a different WAN port.

Firewall > One-To-One NAT (SNAT) > Add Service

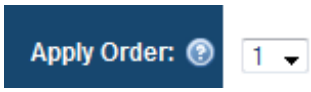
External Address: Forward Address allows you to identify the server to which the protocol/service will be directed. Internet Address - Must be available via the WAN port selected below.



Inbound Interface: Select the WAN interface that will be used for inbound NAT translation OR enter a specific address which will be automatically added to the specified WAN interface (a port may also be specified for more granular control). IMPORTANT: Make sure to select the correct interface or the NAT rule will not work. Match the Internet address to the correct Inbound Interface.


Internal Address:
(Forward Address(es) Must be available via the LAN interface)
(Server load balancing can be accomplished by entering the following xxx.xxx.xxx.yyy-xxx.xxx.xxx.zzz)

Internal Address: Add the internally routed IP address that will serve as the host for the services being directed by the public IP address entered above.



Apply Order: The APPLY ORDER function is used to allow network administrators control which mappings will be applied and in which order based on the current active state of each WAN link. Only one server mapping can be active at any given time, thus the APPLY ORDER variable allows one to control which mapping will be used and to which WAN link it will be bound.

Reset: Reset the rule's settings to their last saved state.

Add/Update: Add or update a firewall rules.

View Services>>: Return to the main One-To-One NAT page.

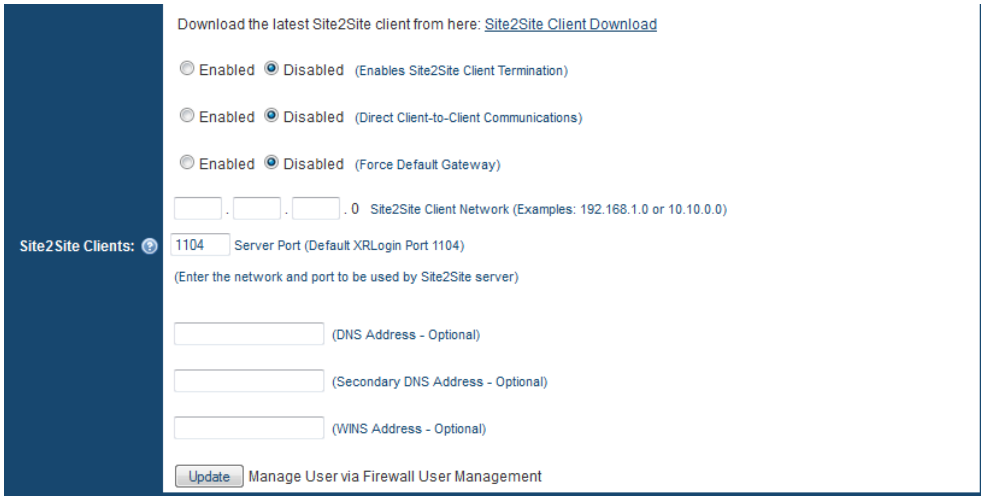
Remote Access Site2Site Client

If you have remote users that wish to access the local network from their home or on the road, the Site2Site software client enables any Windows-compatible computer to connect back to the EdgeXOS appliance.

The client is small and installs in seconds. The configuration is simple ad only requires the IP address of the EdgeXOS appliance (two can be provided for failover) and the port which is being used for client connections. This information can be obtained by the EdgeXOS administrator. Additional step-by-step installation instructions for the client are provided in our Platform Notes section. The client includes 3DES encryption protection using standard SSL tunneling technology, which is an improvement over IPSec based VPNs as they do not have any issues going through hotel firewalls, etc.

To get started simply download the client from the link on the configuration page.

Firewall > EdgeXOS Security > Remote Access Site2Site Client


Download the latest Site2Site client from here: Site2Site Client Download
Enabled Disabled (Enables Site2Site Client Termination)
Enabled Disabled (Direct Client-to-Client Communications)
Enabled Disabled (Force Default Gateway)
. . . 0 Site2Site Client Network (Examples: 192.168.1.0 or 10.10.0.0)
Site2Site Clients:
1104 Server Port (Default XRLogin Port 1104)
(Enter the network and port to be used by Site2Site server)
(DNS Address - Optional)
(Secondary DNS Address - Optional)
(WINS Address - Optional)
Update Manage User via Firewall User Management

Site2Site Clients: To enable remote access to from telecommuters simply download the Site2Site client to the remote system. These clients use 3DES SSL-based tunnels to provide full network acess to remote users. These are certificate-based tunnels with replay protection and additional packet based signature testing for added security. Enable the Site2Site server and enter the network address to be used to dynamically assign addresses to the remote clients. User/passwords are controlled via the User/Device Management section. All secondary LAN networks and static routes will be pushed to the clients.

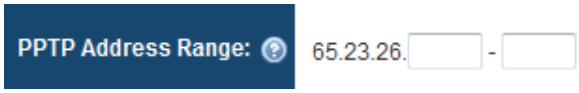
In order for a remote client to connect they must first be defined within the User/Device Management tool. This tool includes an authentication field which is used as the remote users password. If "client-to-client" communication is enabled then two remote users will be able to share network information and potentially connect to each others shared resources. If the "force default gateway" option is used, then all of the remote users traffic will go through the EdgeXOS appliance, i.e. the user will not be able to surf the Internet locally. When defining the client network make sure that it is not part of any local network, including the local LAN IP addresses, this network MUST be separate from any other networks used by the EdgeXOS appliance. The EdgeXOS administrator can use any port they wish for client connections, however keep in mind that many ISPs will block high ports so it is typically recommended to use ports under 1200.

Finally, if you have local resources which should be passed to the remote clients they can be passed using the DNS and WINS fields.

Remote Access PPTP Client

The EdgeXOS platform supports limited PPTP client support for customers not able to utilize our Site2Site client software to establish remote access connectivity.

Firewall > EdgeXOS Security > Remote Access PPTP Client



PPTP Address Range: Enter the IP address pool from which clients will be assigned an IP address. If a user is assigned an address and attempts to reconnect they will receive the same IP address. However upon a server reset, a different address may be allocated.

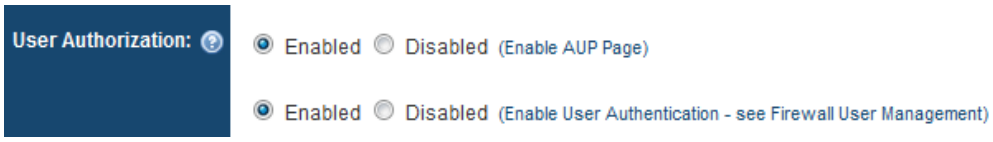
PPTP MTU:
Default 1400
Update
NOTE: PPTP connections are not very secure and can only be made to the primary active connection, the Site2Site client is recommended for greater security.
Example: If WAN1 is active, PPTP will ONLY work acorss the WAN1 interface.
Reset Server
Manage PPTP Users via Firewall User Management

PPTP MTU: Enter the IP address pool from which clients will be assigned an IP address. If a user is assigned an address and attempts to reconnect they will receive the same IP address. However upon a server reset, a different address may be allocated.

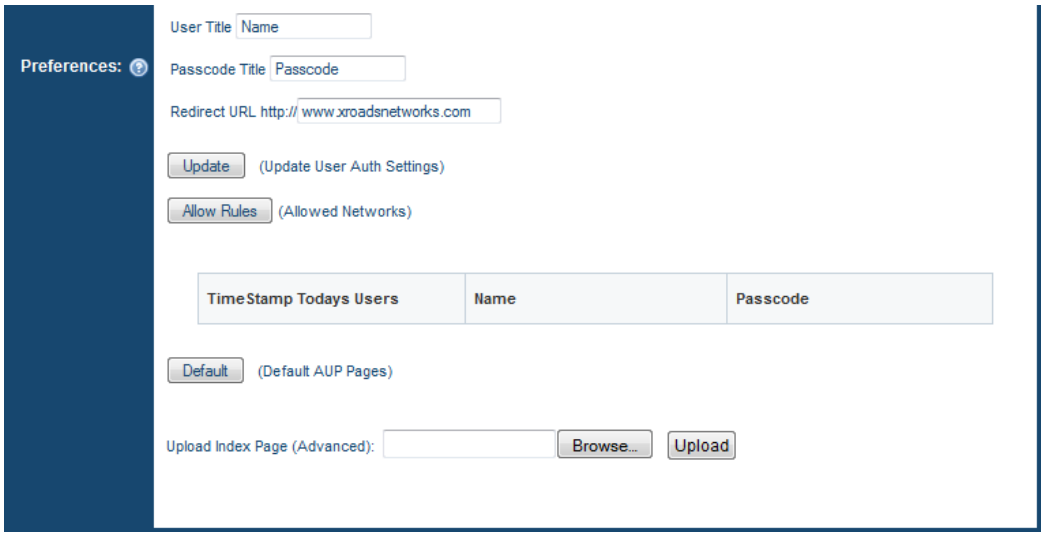
User/Device Access Control (NAC)

This option provides network administrators with the ability to provide a forced login page for end-users which requires either a login or that they select a checkbox in order to continue to utilize Internet services.

Firewall > EdgeXOS Security > User/Device Access Control (NAC)



User Authorization: This feature allows an administrator to require that end-users first get authorized prior to accessing the Internet through the EdgeXOS appliance. This feature currently supports the ability to require AUP acceptance and will be able to perform password based authentication in the future.



Preferences: These settings allow the administrator to direct web site to the initial message, then the post-authorization message. The administrator may also change the name/title of the acceptance strings (User Name or Guest / Passcode or Room Number).

Monitoring and Reporting Capabilities

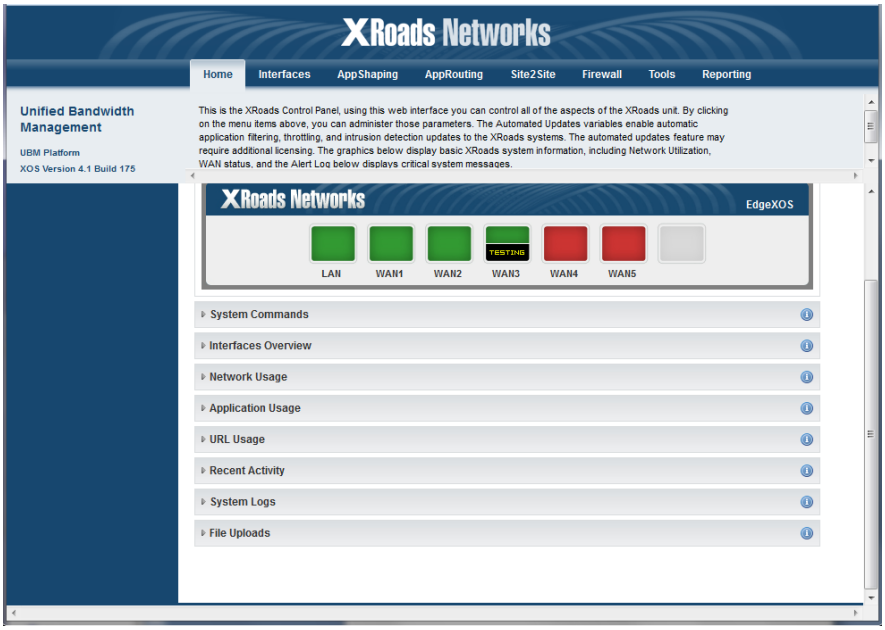
The EdgeXOS platform utilizes XRoads Networks real-time reporting engine XFLOW. XFlow collects traffic data passing through the hardware appliance and produces a number of different reports based on the collected and summarized data.

Dashboard (Home page) Overview

- Dashboard
- System Commands
- Interfaces Overview
- Network Usage
- Application Usage
- URL Usage
- Recent Activity
- System Logs
- File Uploads

Dashboard

The Home page dashboard gives you a quick read on your network.

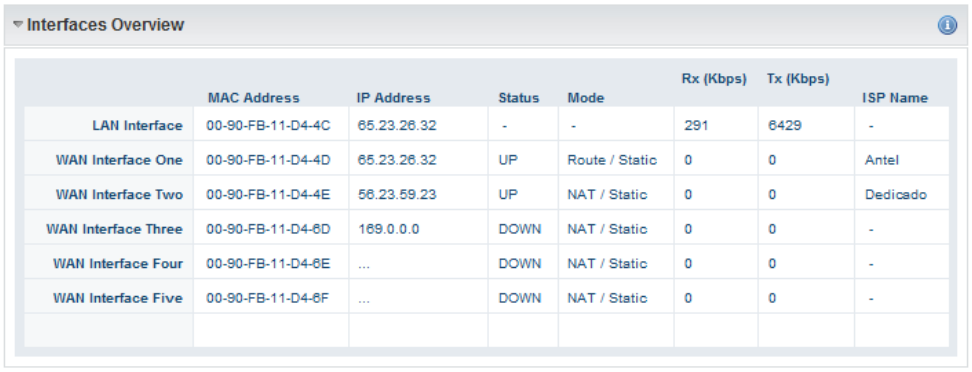

XRoads Networks
Home
Interfaces
AppShaping
AppRouting
Site2Site
Firewall
Tools
Reporting
Unified Bandwidth Management
UBM Platform
XOS Version 4.1 Build 175
This is the XRoads Control Panel, using this web interface you can control all of the aspects of the XRoads unit. By clicking on the menu items above, you can administer those parameters. The Automated Updates variables enable automatic application filtering, throttling, and intrusion detection updates to the XRoads systems. The automated updates feature may require additional licensing. The graphics below display basic XRoads system information, including Network Utilization, WAN status, and the Alert Log below displays critical system messages.
XRoads Networks
EdgeXOS
TESTING
LAN
WAN1
WAN2
WAN3
WAN4
WAN5
System Commands
Interfaces Overview
Network Usage
Application Usage
URL Usage
Recent Activity
System Logs
File Uploads

System Commands

Use this area to save the current configuration, reboot the appliance, and/or commit configuration changes made to interfaces using the Interface menu options:

Interfaces Overview

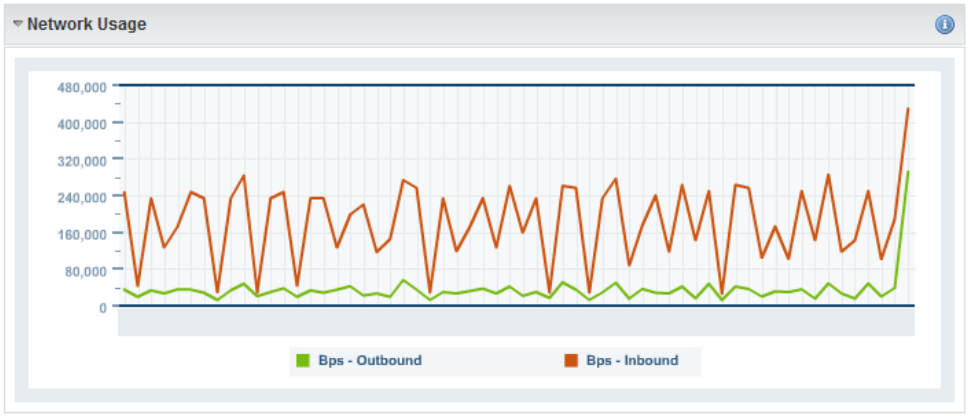
This area provides basic information on all of your configured interfaces, including MAC address, IP address, Status, Mode, RX, TX, and ISP Name:



	MAC Address	IP Address	Status	Mode	Rx (Kbps)	Tx (Kbps)	ISP Name
LAN Interface	00-90-FB-11-D4-4C	65.23.26.32	-	-	291	6429	-
WAN Interface One	00-90-FB-11-D4-4D	65.23.26.32	UP	Route / Static	0	0	Antel
WAN Interface Two	00-90-FB-11-D4-4E	56.23.59.23	UP	NAT / Static	0	0	Dedicado
WAN Interface Three	00-90-FB-11-D4-6D	169.0.0.0	DOWN	NAT / Static	0	0	-
WAN Interface Four	00-90-FB-11-D4-6E	...	DOWN	NAT / Static	0	0	-
WAN Interface Five	00-90-FB-11-D4-6F	...	DOWN	NAT / Static	0	0	-

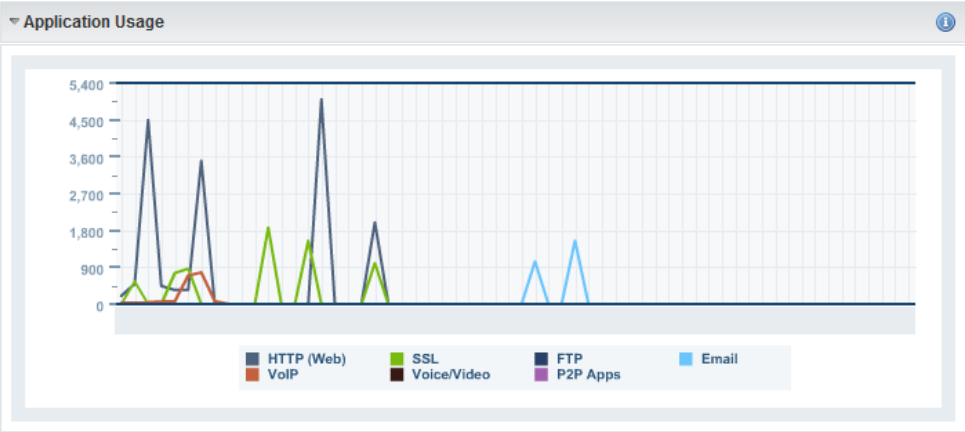
Network Usage

This real time network usage report provides the throughput rate in bits per second, in and out of the device between the LAN and WAN interfaces. To view individual WAN traffic, go to the **Reporting** tab:



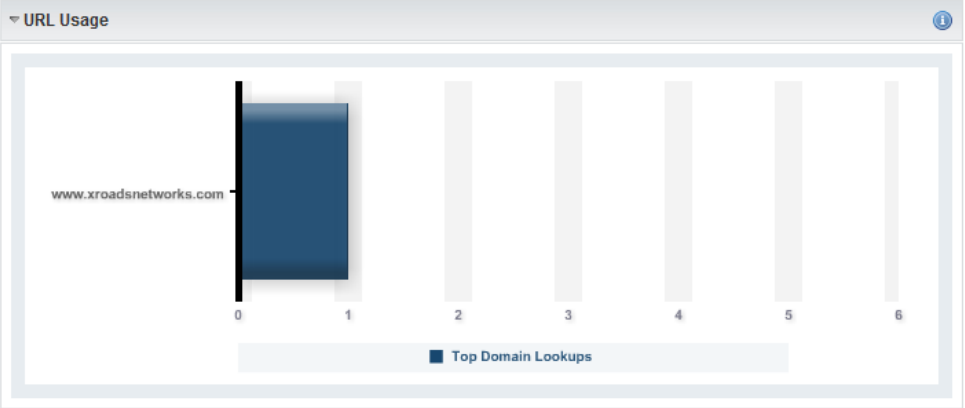
Application Usage

This real time application usage report provides the total throughput rate, in bits per second, per application being forwarded through the appliance. To view individual WAN traffic, go to the **Reporting** tab:



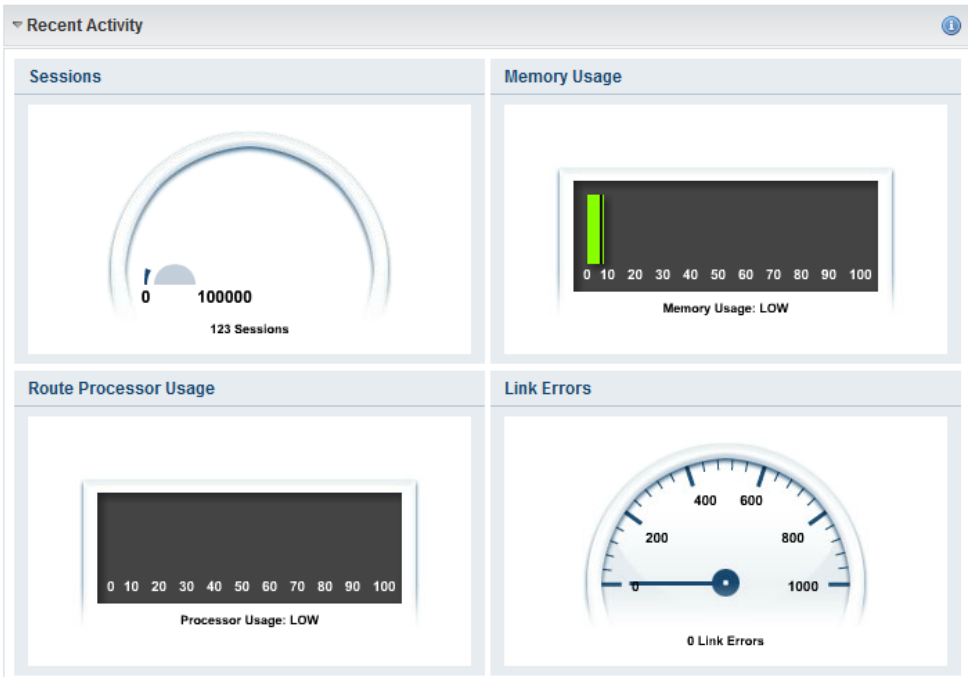
URL Usage

This real time URL usage report provides the top sites and domains being access by end-users going through the system. This information is collected using DNS queries:



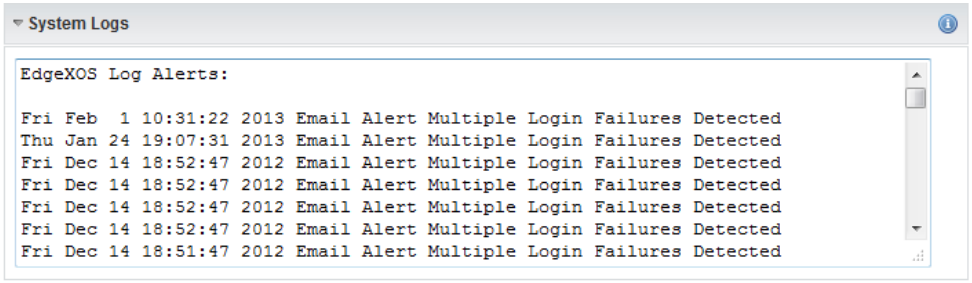
Recent Activity

This area offers four real-time, dynamic, charts of network activity including Sessions, Memory Usage, Route Processor Usage, and Link Errors:



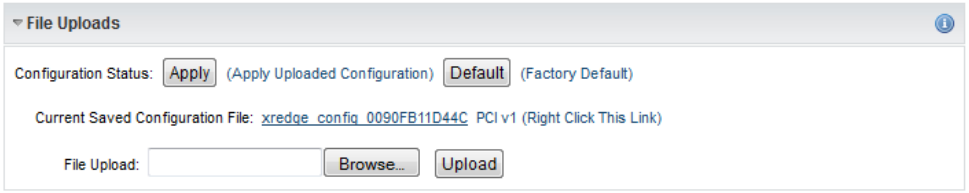
System Logs

This area opens a window to the system log that provides high alert notices for events including: network outages, security issues, report generation, reboots, and threshold monitoring. The alerts are listed in order of time with the most recent at the top:


System Logs
EdgeXOS Log Alerts:
Fri Feb 1 10:31:22 2013 Email Alert Multiple Login Failures Detected
Thu Jan 24 19:07:31 2013 Email Alert Multiple Login Failures Detected
Fri Dec 14 18:52:47 2012 Email Alert Multiple Login Failures Detected
Fri Dec 14 18:52:47 2012 Email Alert Multiple Login Failures Detected
Fri Dec 14 18:52:47 2012 Email Alert Multiple Login Failures Detected
Fri Dec 14 18:52:47 2012 Email Alert Multiple Login Failures Detected
Fri Dec 14 18:51:47 2012 Email Alert Multiple Login Failures Detected

File Uploads

Use this panel to upload the latest firmware or the latest configuration file updates. Save the current configuration by clicking the configuration file URL link and copying the configuration to a standard text editor for backup purposes:



XFlow Reporting Engine (XRE)

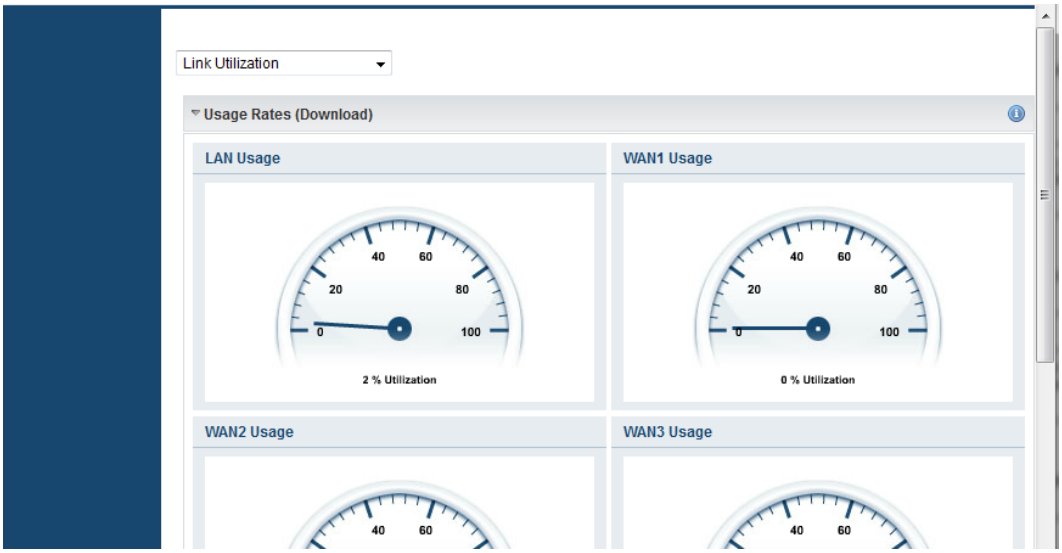
This is the XRoads Reporting control panel; from here you can review the system logs, configure the syslog server address, create alert notifications via email and/or pager, and display WAN statistics (bytes [1 byte = 8 bits] per second) and latency / packet loss information for each configured critical network.

- Link Utilization
- Historical WAN Reporting
- SLA Reporting
- XFlow Bandwidth Usage
- XFlow Graphical Reports
- XFlow Control
- MVP Subnet Reporting
- Web Filter URL Reporting
- Web Filter Live Reporting
- Web Filter Usage Reporting
- Device Monitoring

- Firewall Logs
- System Logs

Link Utilization

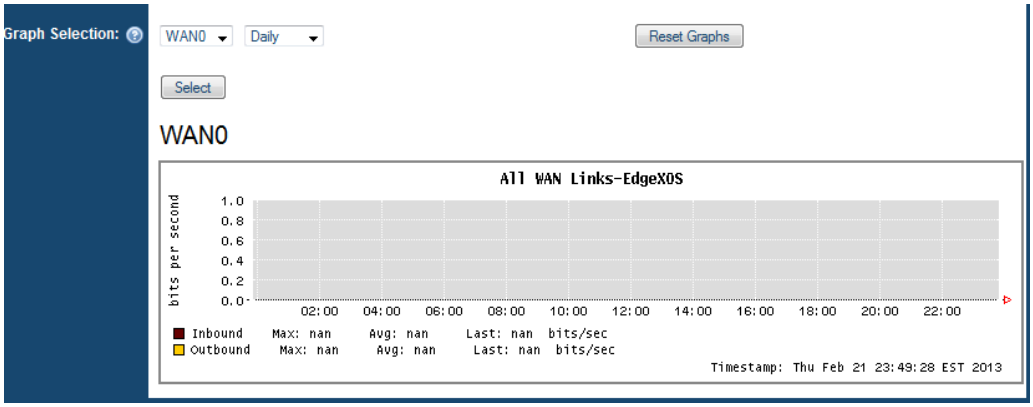
This graph shows the amount of traffic going through the appliance based on the defined link rates set under the Interfaces configuration. Example: If the link rate for WAN1 is set to 10Mbps, and 1Mbps is being used, then the Link Utilization for WAN1 will be 10%.



Historical WAN Reporting

These graphs provide long-term utilization information, this data is summarized and averaged so it will not show bandwidth spikes, however it will provide a good understanding of utilization over time. For shorter term usage information see the Dashboard.

Reporting > Reporting > Historical WAN Reporting

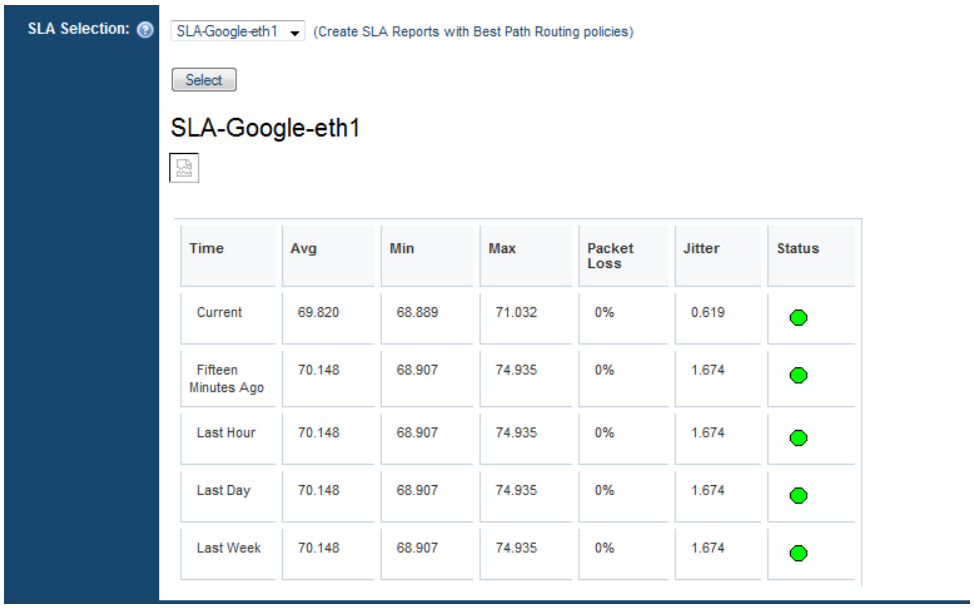


Graph Selection: Select either the WAN interface you wish to view, or select a defined critical network to view latency and packet loss. You can define critical networks under the EdgeBPR menu.

SLA Reporting

These reports enable network administrates to see how each of their WAN links are performing and to determine if the links are meeting their require service level agreements. If the graph does not appear (as seen below), simply wait for approx. 15 minutes while the data is being collected and then it will appear.

Reporting > Reporting > SLA Reporting



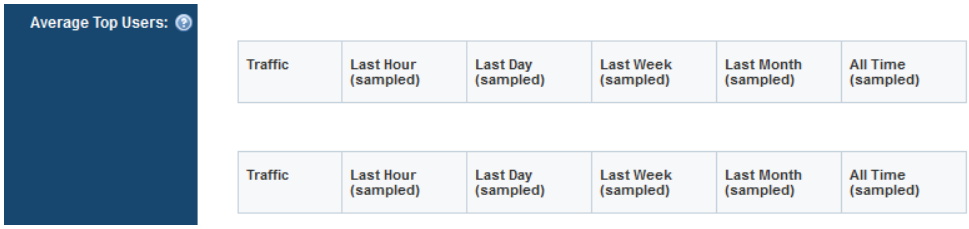
Time	Avg	Min	Max	Packet Loss	Jitter	Status
Current	69.820	68.889	71.032	0%	0.619	
Fifteen Minutes Ago	70.148	68.907	74.935	0%	1.674	
Last Hour	70.148	68.907	74.935	0%	1.674	
Last Day	70.148	68.907	74.935	0%	1.674	
Last Week	70.148	68.907	74.935	0%	1.674	

SLA Selection: Select either the WAN interface you wish to view, or select a defined critical network to view latency and packet loss. You can define critical networks under the EdgeBPR menu.

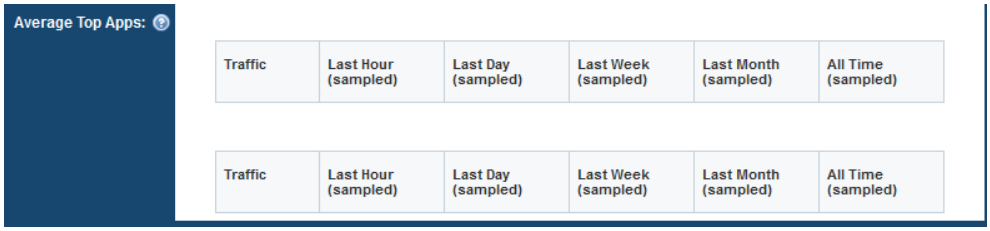
XFlow Bandwidth Usage

Using data sampling, the EdgeXOS appliance can provide insight as to which users are taking up the most bandwidth and which applications they are using. This can be helpful for identifying abusive users and/or top users of bandwidth in order to determine whether additional throttling or more bandwidth resources are required.

Reporting > Reporting > XFlow Bandwidth Usage



Average Top Users: This is a listing of the top users based on the average packet size data collected by the XFlow reporting engine. By default XFlow takes samples of network data over time in order to determine top users and applications. Top downloads are those users which are using the most bandwidth from the Internet back to their network devices. Top uploads are thise users which are sending the most data from their network devices (servers) to the Internet.



Average Top Apps: This is a listing of the top applications based on the average packet size data collected by the XFlow reporting engine. By default XFlow takes samples of network data over time in order to determine top users and applications. Top inbound is the amount of application data which is coming from the Internet. Top outbound are those applications which are sending the most data from the LAN out to the Internet.

XFlow Graphical Reports

This is the graphical version of the utilization reports.

Reporting > Reporting > XFlow Graphical Reports

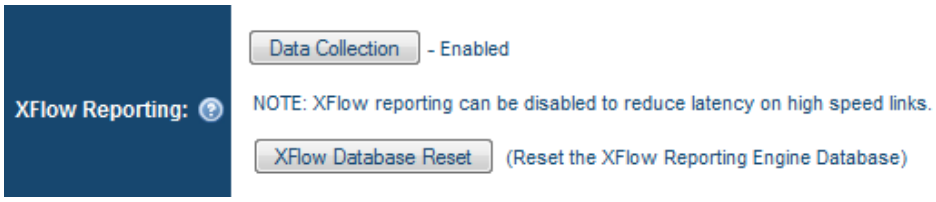
Traffic Flows:
Top Users
(Select Report)
Inbound
(Direction)
Generate Report
NOTE: Generating a report may take a moment, please wait for completion.
Reset Flow Data
Flow Data Last Reset: Thu Jan 3 14:51:28 2013
Current Time: Thu Feb 21 23:54:17 2013

Traffic Flows: Report on the top users of network bandwidth and which applications are being used by those end-users.

XFlow Control

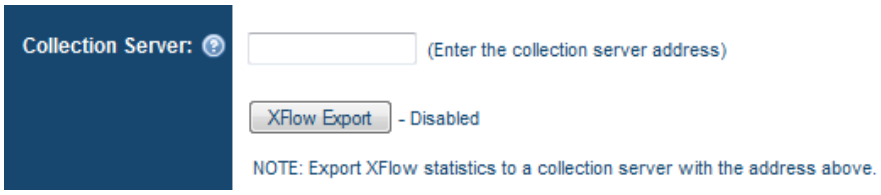
Used to enable XFlow packet capture and data summarization, if this is disabled, many of the reports in the reporting tab will not function.

Reporting > Reporting > XFlow Control

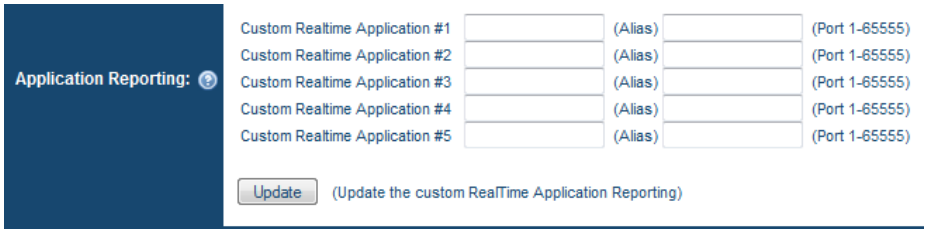

XFlow Reporting:
Data Collection
- Enabled
NOTE: XFlow reporting can be disabled to reduce latency on high speed links.
XFlow Database Reset
(Reset the XFlow Reporting Engine Database)

XFlow Reporting: The XFLOW network reporting module provides application and end-user reporting. XFlow works by sampling network usage over time in order to determine top users and applications. XFlow may also perform full packet capture which provides greater detail and more accurate information, however at times this level of data collection can be processor intensive, thus the administrator has the ability to disable these collection tasks in order to improve traffic throughput when under heavy load conditions.

Reporting > Reporting > XFlow Control


Collection Server:
(Enter the collection server address)
XFlow Export
- Disabled
NOTE: Export XFlow statistics to a collection server with the address above.

Collection Server: The collection server is a host which can receive and log XFlow data and typically includes some utility for viewing the data in a formatted manner. The XFlow data has been formatted to fit the OpenSource SFlow model. To obtain an SFlow collection server, please contact www.sflow.org.

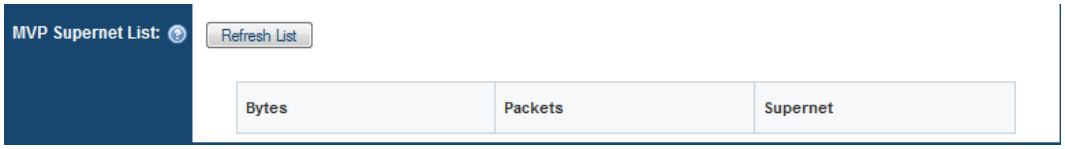


Application Reporting: Customize the application reporting found on the Dashboard.

MVP Subnet Reporting

Used to display the top destinations your end-users are going to. This can be used with Best Path Routing to re-route traffic in order to spreads the load manually.

Reporting > Reporting > MVP Supernet Reporting

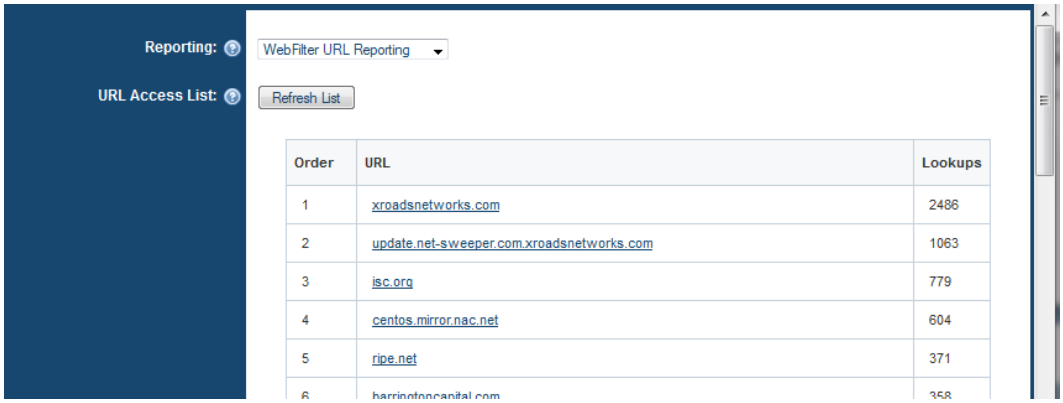


MVP Supernet List: This is a list of top supernet accessed by LAN users.

Web Filter URL Reporting

When the web filter is enabled, this report will show the top websites accessed by internal users.

Reporting > Reporting > Web Filter URL Reporting

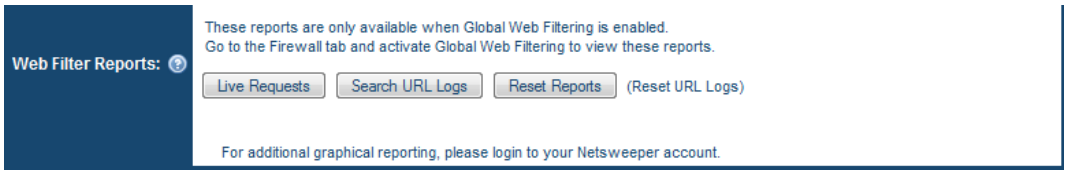


URL Access List: Real-time reporting of the current URL requests being made by users. This listing is continuously updated as new URL requests are made.

Web Filter Live Reporting

When the web filter is enabled, this report will show the recent websites accessed by internal users.

Reporting > Reporting > Web Filter Live Reporting

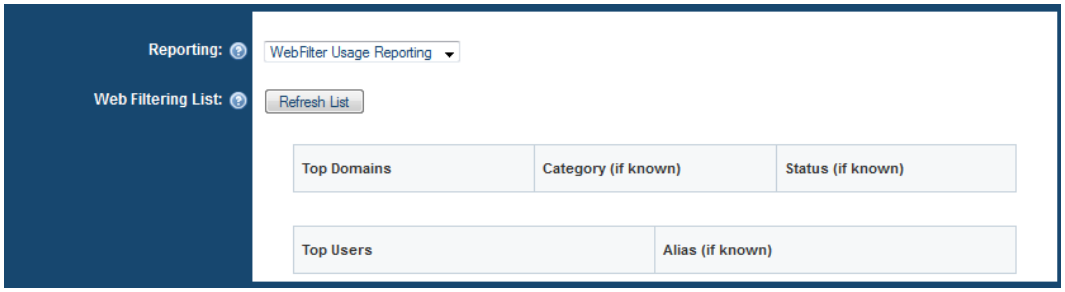

Web Filter Reports:
These reports are only available when Global Web Filtering is enabled.
Go to the Firewall tab and activate Global Web Filtering to view these reports.
Live Requests
Search URL Logs
Reset Reports
(Reset URL Logs)
For additional graphical reporting, please login to your Netsweeper account.

Web Filter Reports: The web reporting module provide some basic web-based reporting of live web requests and top site visitations. For more detailed web reporting, please login to the content control center at http://myfilter.xroadsnetworks.com.

Web Filter Usage Reporting

When the web filter is enabled, this report will show the top users accessing websites.

Reporting > Reporting > Web Filter Usage Reporting

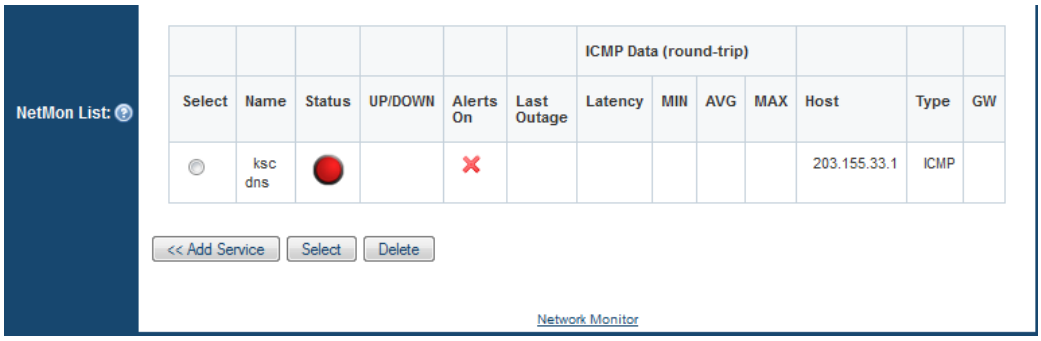


Web Filtering List: These reports provide the top domains accessed and the users making the most requests through the global web filter built-in to the firewall feature set. The global web filter must be enabled to view these reports.

Device Monitoring

Use this feature to monitor internal devices and send out alerts when the monitored device is not responding.

Reporting > Reporting > Device Monitoring

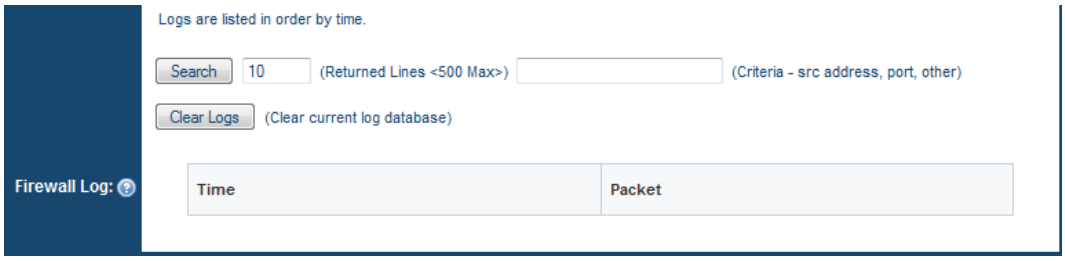


NetMon List: This list contains all of the current network nodes that are being monitored by the EdgeXOS router.

Firewall Logs

This feature, enabled via the Firewall log function when creating new firewall rules, allows an administrator to troubleshoot network traffic by logging the full packet header information for those packets which match the defined firewall rule. See the Firewall section to see how to enable this logging.

Reporting > Reporting > Firewall Logs



Firewall Log: This is a listing of the packets logged using the firewall logging function. You may search through the list using fields above.

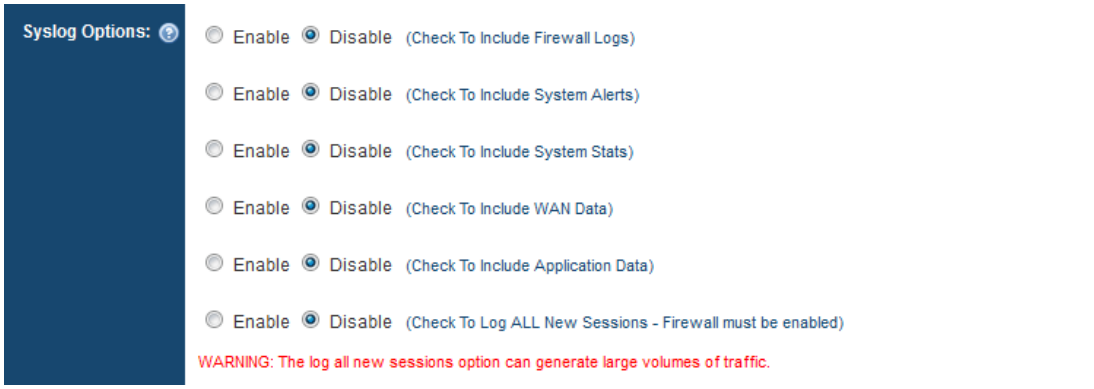
System Logs

These logs show common system alerts and notices. They are automatically created based on changes to the EdgeXOS appliance.

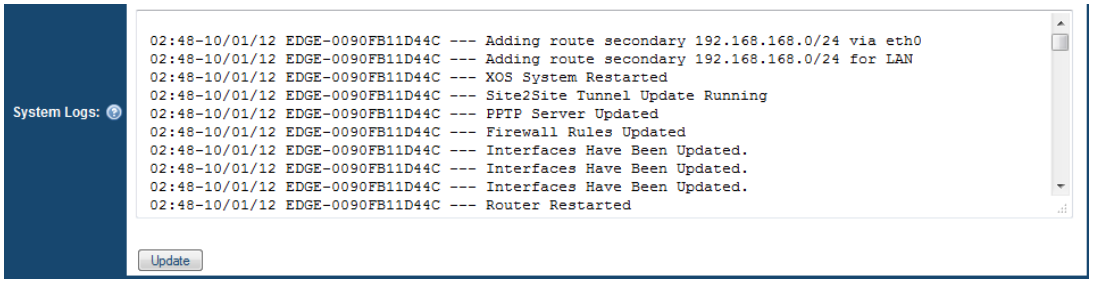
Reporting > Reporting > System Logs

Syslog Server: Define the IP address of a syslog server which is to receive outage and system notification syslog messages.

Reporting > Reporting > System Logs


Syslog Options:
Enable Disable (Check To Include Firewall Logs)
Enable Disable (Check To Include System Alerts)
Enable Disable (Check To Include System Stats)
Enable Disable (Check To Include WAN Data)
Enable Disable (Check To Include Application Data)
Enable Disable (Check To Log ALL New Sessions - Firewall must be enabled)
WARNING: The log all new sessions option can generate large volumes of traffic.

Syslog Options: When enabled any firewall logs will automatically be sent out via the syslog server. This is helpful for remote monitoring of various firewall access privileges.


System Logs:
02:48-10/01/12 EDGE-0090FB11D44C --- Adding route secondary 192.168.168.0/24 via eth0
02:48-10/01/12 EDGE-0090FB11D44C --- Adding route secondary 192.168.168.0/24 for LAN
02:48-10/01/12 EDGE-0090FB11D44C --- XOS System Restarted
02:48-10/01/12 EDGE-0090FB11D44C --- Site2Site Tunnel Update Running
02:48-10/01/12 EDGE-0090FB11D44C --- PPTP Server Updated
02:48-10/01/12 EDGE-0090FB11D44C --- Firewall Rules Updated
02:48-10/01/12 EDGE-0090FB11D44C --- Interfaces Have Been Updated.
02:48-10/01/12 EDGE-0090FB11D44C --- Interfaces Have Been Updated.
02:48-10/01/12 EDGE-0090FB11D44C --- Interfaces Have Been Updated.
02:48-10/01/12 EDGE-0090FB11D44C --- Router Restarted
Update

System Logs: This is a list of the system logs sent by the XRoads syslog server.

Tools

- Registration
- SNMP/XGM Control
- Virtual Technician
- Time/Date Setting
- Remote Access
- Admin Access
- Email Alerts
- Ping
- Port Speed / Duplex
- Route Table
- Arp Table
- Hardware High Availability

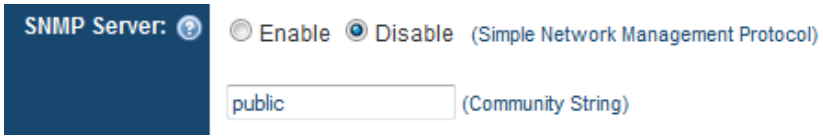
Registration

To register your XRoads unit with technical support, see Registration.

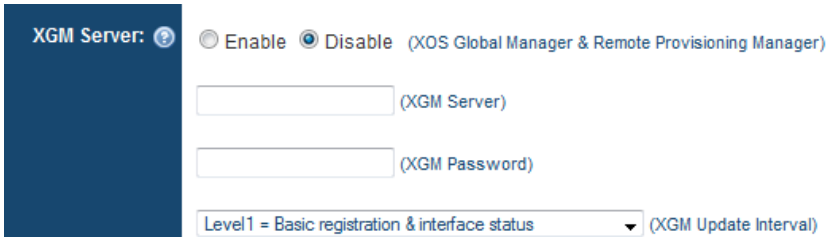
SNMP/XGM Control

Choose **SNMP/XGM** in the **Tools** tab **EdgeXOS Tools** menu to open this page of configuration options

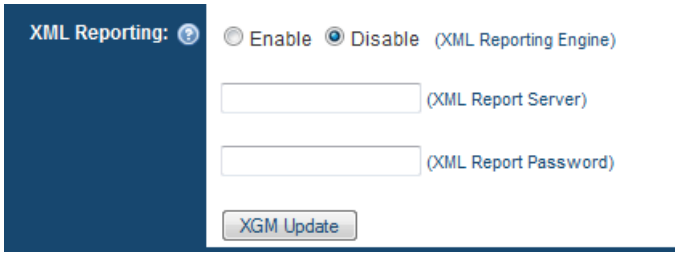
Tools > EdgeXOS Tools > SNMP/XGM Control



SNMP Server: Enable to allow SNMP request to the EdgeXOS appliance, via port 161.



XGM Server: The XGM (XRoads Global Manager) is a server-based application which can be used to collect data from the EdgeXOS appliances. The RPM (Remote Provisioning Manager) module of the XGM system also provides the ability to automatically update the EdgeXOS appliance remotely and can be used to update multiple systems at the same time.

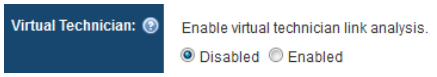


XML Reporting: The XML Reporting Engine is designed to allow administrators to create their own detailed reports which can be completely customized. Additionally, these reports can be automatically generated in PDF format and emailed to any end-user. This functionality requires Microsoft Excel 2007 or later.

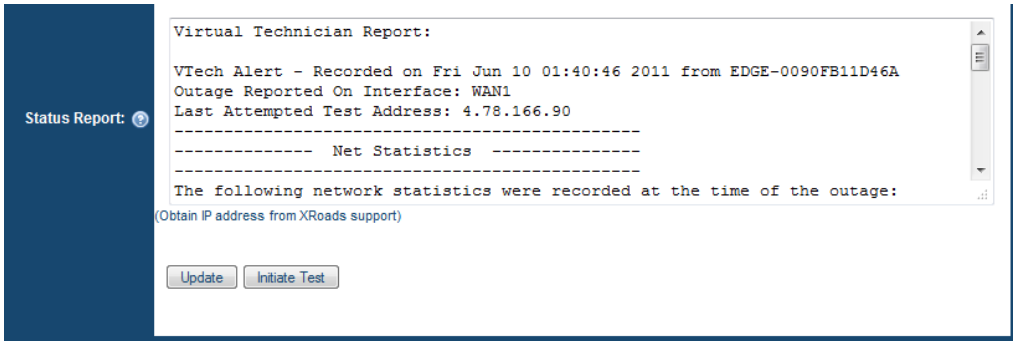
Virtual Technician

Choose **Virtual Technician** in the **Tools** tab **EdgeXOS Tools** menu to open this page of configuration options

Tools > EdgeXOS Tools > Virtual Technician



Virtual Technician: The Virtual Technician provides a set of automated tools to assist in troubleshooting connectivity problems when an error occurs. The results of these automated tests can then be emailed to the network administrator and support departments of the service provider.


Status Report:
Virtual Technician Report:
VTech Alert - Recorded on Fri Jun 10 01:40:46 2011 from EDGE-0090FB11D46A
Outage Reported On Interface: WAN1
Last Attempted Test Address: 4.78.166.90
---------- Net Statistics ----------
The following network statistics were recorded at the time of the outage:
(Obtain IP address from XRoads support)
Update
Initiate Test

Status Report: This shows the status of a failed WAN link and provides a summary of the problem.

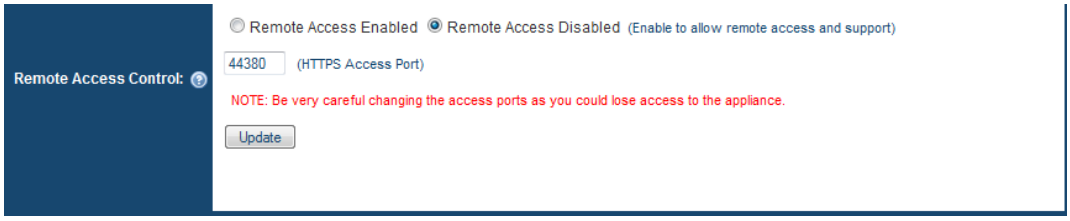
Time/Date Setting

To set your system's time and date, see Setting Time/Date.

Remote Access

Choose **Remote Access** in the **Tools** tab **EdgeXOS Tools** menu to open this page of configuration options.

Tools > EdgeXOS Tools > Remote Access


Remote Access Control:
Remote Access Enabled
Remote Access Disabled
(Enable to allow remote access and support)
44380
(HTTPS Access Port)
NOTE: Be very careful changing the access ports as you could lose access to the appliance.
Update

Remote Access Control: Control access privileges for USER based access.

Admin Access

To update your administrative password, see Setting the Password.

Email Alerts

To manage your email alerts, see Setting Email Alerts.

To add an email alert, see Add an Email Alert.

Ping

Choose **Ping** in the **Tools** tab **EdgeXOS Tools** menu to open this page of configuration options.

Tools > EdgeXOS Tools > Ping

Ping: This tool allows you to perform a ping test to a remote network device or address.

Port Speed / Duplex

To set your NIC port speed and duplex, see Setting NIC Speed/Duplex.

Route Table

Choose **Route Table** in the **Tools** tab **EdgeXOS Tools** menu to open this page of configuration options.

Tools > EdgeXOS Tools > Route Table

Route: This tool allows you to view the current status of the XRoads routing table.

Arp Table

Choose **Arp Table** in the **Tools** tab **EdgeXOS Tools** menu to open this page of configuration options.

Tools > EdgeXOS Tools > Arp Table

ARP: This tool allows you to view the current status of the XRoads ARP table.

ARP Update: This tool allows you to view the current status of the XRoads ARP table.

Hardware High Availability

Choose **Hardware High Availability** in the **Tools** tab **EdgeXOS Tools** menu to open this page of configuration options.

Tools > EdgeXOS Tools > Hardware High Availability

High Availability: Use this tool to setup High Availability between two XRoads units. High Availability ensures that if one of the XRoads units fail, the backup unit will take over all connectivity. To configure this function, enter the HA addresses for the primary and secondary units or use the default - recommended. Then enter the serial number for your secondary unit (found on the LAN interface page). Select PRIMARY or SECONDARY from the dropdown menu depending on the unit. Select how often the two units will sync themselves and finally select whether to activate HA. Activating HA will begin the transfer of all configuration information from your primary unit to the secondary unit at the selected interval. Be aware that the secondary unit will be completely inaccessible except for the HA port address.

Appendix A - Factory Default

If you are locked out of the EdgeXOS appliance because the IP address has been changed to some unknown address, or the password is no longer working because someone changed it or mistyped, the EdgeXOS appliance can be reset to factory defaults using the following procedure.

Use the console port to default the appliance, you can either default the entire configuration or simple the password.

Console access can be obtained via the console port:

Newer console ports use an interface that looks like an Ethernet interface, but it will be correctly labeled as a CONSOLE port. Be sure not to confuse the two.

Step One

Connect to the console port of the EdgeXOS appliance using a console cable and a terminal program (HyperTerminal is recommended for MS Windows).

```
Welcome to XRoads Edge
-----Command Menu-----

1-Password Default
2-Full System Default

Enter Selection (1-2)? _
```

Step Two

Once connected, login using "default" and password "confirmdefault"

```
Welcome to XRoads Edge
-----Command Menu-----

1-Password Default
2-Full System Default

Enter Selection (1-2)? 2

Are you sure you want to default the router? (Yes/No)? Yes
```

Step Three

Select the appropriate reset function. If you are unable to ping the device, selecting factory default will reset the LAN address back to 192.168.168.254.

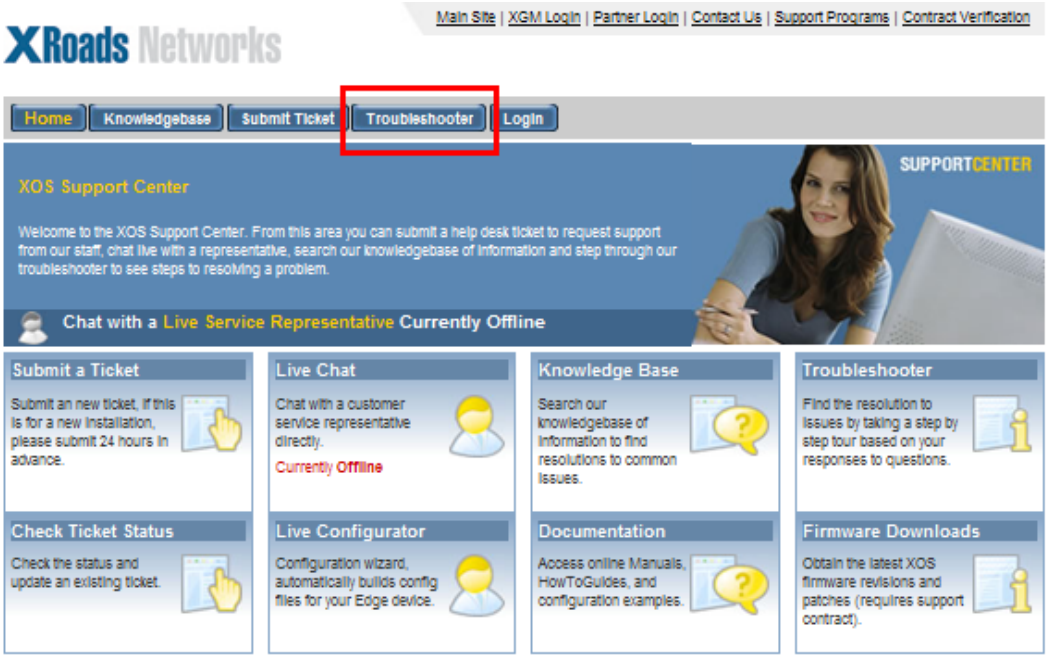
```
XRoads Edge Router (Console Access)
Version X.0+

xroads login: default
Password: _
```

Enter "Yes" and press the RETURN key to begin the reset process.

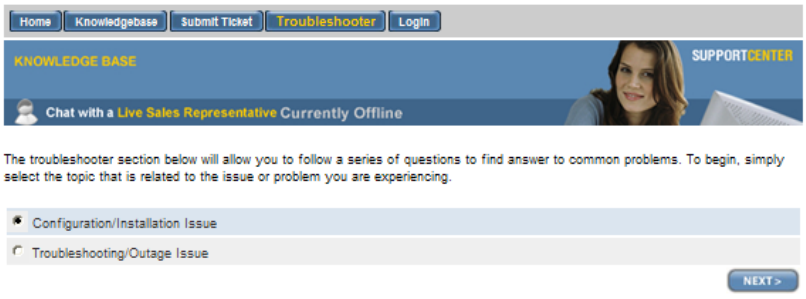
After approximately three-five minutes the appliance should be reset and replying to the 192.168.168.254 address, assuming your computer is on the 192.168.168.0 network.

Appendix B – Troubleshooting

XRoads Networks has developed a specific aspect of our MYXROADS site which is designed to provide our customers with dedicated access to troubleshooting support, please visit www.myxroads.com for more details.


Main Site | XGM Login | Partner Login | Contact Us | Support Programs | Contract Verification
XRoads Networks
Home
Knowledgebase
Submit Ticket
Troubleshooter
Login
XOS Support Center
SUPPORTCENTER
Welcome to the XOS Support Center. From this area you can submit a help desk ticket to request support from our staff, chat live with a representative, search our knowledgebase of information and step through our troubleshooter to see steps to resolving a problem.
Chat with a Live Service Representative Currently Offline
Submit a Ticket
Submit an new ticket. If this is for a new installation, please submit 24 hours in advance.
Live Chat
Chat with a customer service representative directly.
Currently Offline
Knowledge Base
Search our knowledgebase of information to find resolutions to common issues.
Troubleshooter
Find the resolution to issues by taking a step by step tour based on your responses to questions.
Check Ticket Status
Check the status and update an existing ticket.
Live Configurator
Configuration wizard, automatically builds config files for your Edge device.
Documentation
Access online Manuals, HowToGuides, and configuration examples.
Firmware Downloads
Obtain the latest XOS firmware revisions and patches (requires support contract).

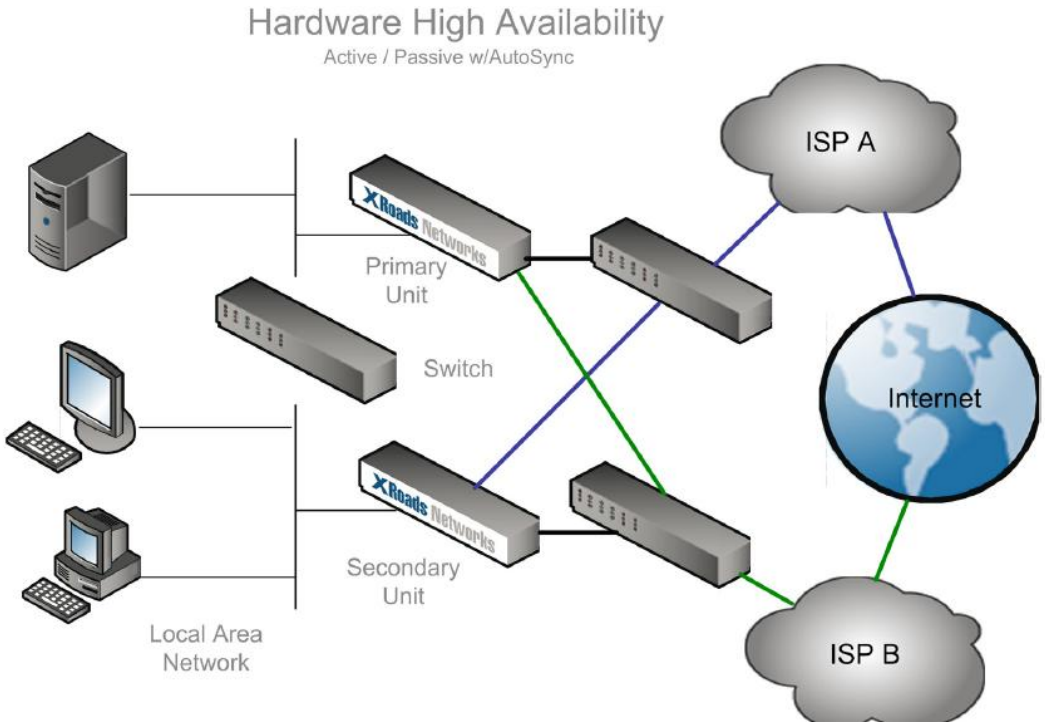
The troubleshooter steps you through various issues and attempts to provide a simple solution to the problem:


Home
Knowledgebase
Submit Ticket
Troubleshooter
Login
KNOWLEDGE BASE
SUPPORTCENTER
Chat with a Live Sales Representative Currently Offline
The troubleshooter section below will allow you to follow a series of questions to find answer to common problems. To begin, simply select the topic that is related to the issue or problem you are experiencing.
Configuration/Installation Issue
Troubleshooting/Outage Issue
NEXT>

Appendix C - Hardware High Availability (HA) Configuration

The EdgeXOS HA (High Availability) module enables the ability of the EdgeXOS appliance to failover from a primary hardware unit to a secondary hardware unit in the case of a hardware failure of the primary unit. This module ensures hardware redundancy for mission critical networking.

Below is a basic diagram of how two EdgeXOS appliances can be configured in HA mode. This diagram assumes the use of the LAN port for the HA testing between the two units.



Either the LAN or WAN5 may be used for HA failover testing. The tests performed are simple ICMP tests to specific HA addresses assigned to each appliance. It is important that these addresses are not currently in use by the customer.

NOTE: It is critical that whichever port is selected for HA testing that the port remain available at all times and that each port is able to communicate with the other at all times. Any loss of

communication would trigger the HA module to failover to the secondary unit. Failover occurs over a period of 60 seconds.

Setup Procedure

The configuration process for the HA module is fairly simple, however it must be followed exactly or the failover will not initialize correctly.

NOTE: Once the configuration has been sync'd the HA screen will display a SYNC'd message. At this point the HA failover module is now "armed" and ready.

(1) Make sure the secondary unit is in its default state.

(2) Configure the HA parameters (see instructions below) on both the primary and secondary unit via the TOOLS menu option via the web interface control. Make sure to leave both HA modules in INACTIVE mode at this time.

(3) Click the save button on both units in order to save the running configuration.

(4) Connect all of the appropriate cables on the WAN and LAN side of the appliances. Make sure that you have good Ethernet layer connectivity by check the Ethernet link lights.

(5) Enable the HA module on the PRIMARY unit, then check to make sure that you are able to ping the HA IP address on the primary unit.

(6) Once you have confirmed that you have a good, pingable link on the primary unit, enable the HA mode on the secondary unit.

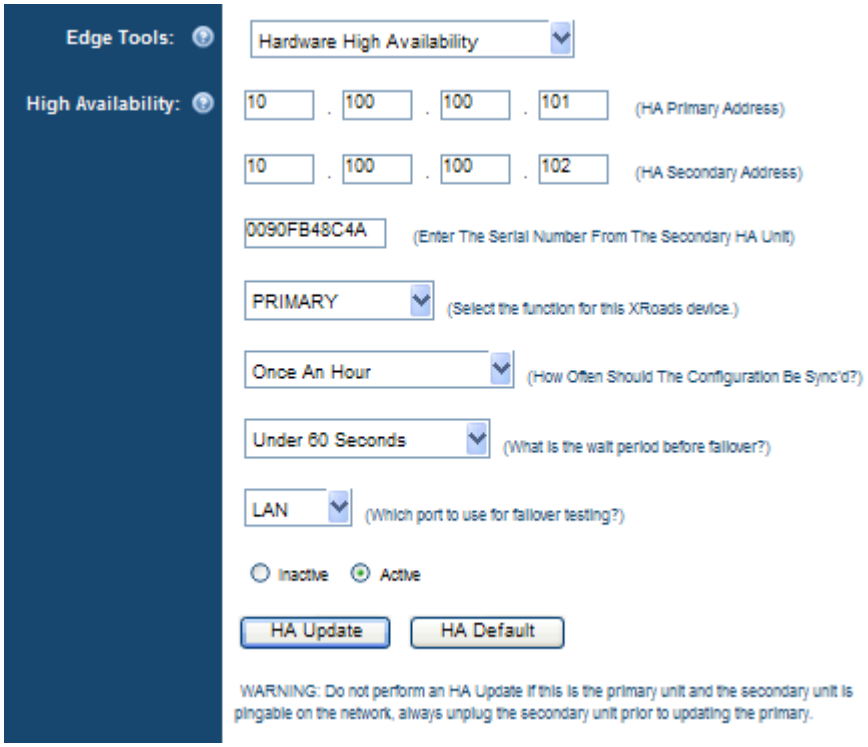
(7) Failover can not occur until the secondary unit has automatically obtained the configuration information from the primary unit. This occurs at the designated sync interval.

NOTE: Once the configuration has been sync'd the HA screen will display a SYNC'd message. At this point the HA failover module is now "armed" and ready.

Primary Unit Configuration

To configure the primary appliance for failover, go to the Tools menu and select the High Availability option from the drop-down menu.

The screen below provides an example of how one might configure the HA module.


Edge Tools:
Hardware High Availability
High Availability:
10 . 100 . 100 . 101
(HA Primary Address)
10 . 100 . 100 . 102
(HA Secondary Address)
0090FB48C4A
(Enter The Serial Number From The Secondary HA Unit)
PRIMARY
(Select the function for this XRoads device.)
Once An Hour
(How Often Should The Configuration Be Sync'd?)
Under 60 Seconds
(What is the wait period before failover?)
LAN
(Which port to use for failover testing?)
Inactive
Active
HA Update
HA Default
WARNING: Do not perform an HA Update if this is the primary unit and the secondary unit is pingable on the network, always unplug the secondary unit prior to updating the primary.

HA Primary Address – This is the address that will be assigned to the primary appliances network interface. The interface it is assigned to is selected below.

HA Secondary Address – This is the address that is assigned to the secondary appliance. The secondary will use this address when performing ICMP testing to the primary address.

Serial Number – This is the serial number that the primary uses to verify the secondary when the configuration information is requested for sync'ing.

Select Function – This parameter is used to determine which device is currently being configured.

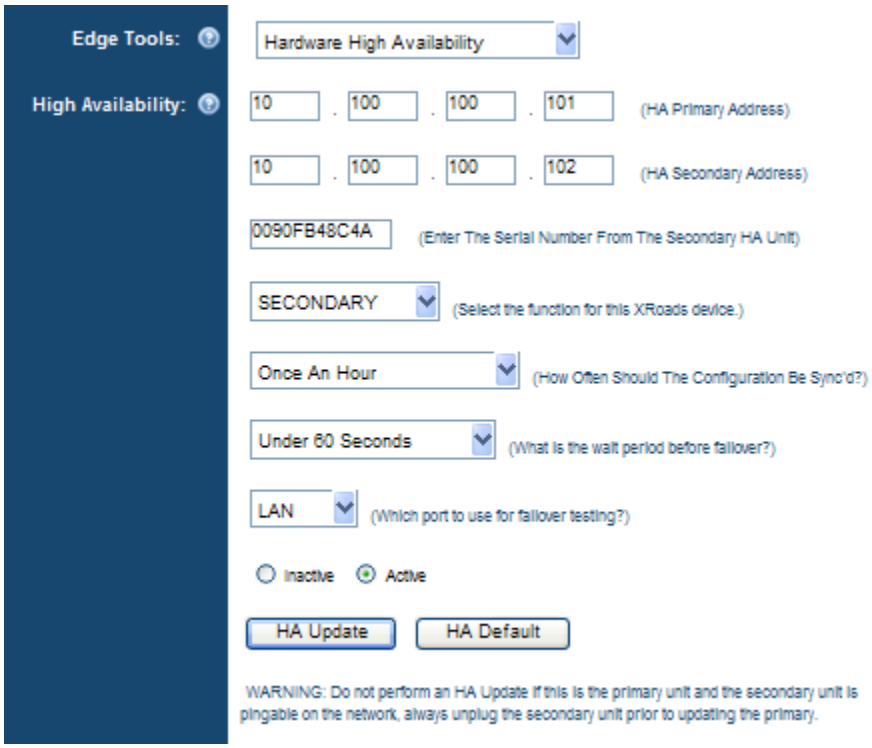
Port – This option determines which port will be used for the HA testing, make sure to use the same port on both appliances.

Inactive / Active – Determines the current state of the HA mode.

Secondary Unit Configuration

To configure the secondary appliance for failover, go to the Tools menu and select the High Availability option from the drop-down menu.

The screen below provides an example of how one might configure the HA module.


Edge Tools:
Hardware High Availability
High Availability:
10 . 100 . 100 . 101
(HA Primary Address)
10 . 100 . 100 . 102
(HA Secondary Address)
0090FB48C4A
(Enter The Serial Number From The Secondary HA Unit)
SECONDARY
(Select the function for this XRoads device.)
Once An Hour
(How Often Should The Configuration Be Sync'd?)
Under 60 Seconds
(What is the wait period before failover?)
LAN
(Which port to use for failover testing?)
Inactive
Active
HA Update
HA Default
WARNING: Do not perform an HA Update if this is the primary unit and the secondary unit is pingable on the network, always unplug the secondary unit prior to updating the primary.

HA Primary Address – This is the address that will be assigned to the primary appliances network interface. The interface it is assigned to is selected below.

HA Secondary Address – This is the address that is assigned to the secondary appliance. The secondary will use this address when performing ICMP testing to the primary address.

Serial Number – This is the serial number that the primary uses to verify the secondary when the configuration information is requested for sync'ing.

Select Function – This parameter is used to determine which device is currently being configured.

Port – This option determines which port will be used for the HA testing, make sure to use the same port on both appliances.

Inactive / Active – Determines the current state of the HA mode.

Post Failover Procedures

After a failover has been detected the secondary unit will take over all traffic flow functions and will also assume the primary systems MAC addresses. It is critical that the primary not be re-enabled after this has occurred as it will cause other network problems.

Upon a primary failure, always remove the primary unit from the network as soon as possible so as to minimize any potential problems with that unit. Obtain a replacement unit by contacting XRoads Networks and obtaining an RMA for that unit.

Follow these procedures to reset the HA mode after a failure has occurred:

NOTE: This should be done after hours as it will cause downtime.

Step 1) Shutdown and remove the primary (non-functioning) unit. Prepare the NEW primary unit by installing the configuration file and confirm that the configuration is correct.

Step 2) Login to the secondary unit and click the HA Update. This will reset the secondary back to a default mode (the previously sync'd configuration will be deleted) and all traffic will stop.

Step 3) Install the new primary unit and bring online. Test all functionality and confirm a good installation. Make sure to Save and backup the configuration when ready.

Step 4) Setup the primary HA service once again using the steps outlined above.

Step 5) The secondary unit will begin testing the primary once again and will attempt to sync the configuration once the primary is online.

Disabling HA Mode

Step 1) Access the web interface of the secondary unit through the HA IP address.

Step 2) Click the HA Default button.

Step 3) Power down the secondary unit.

Step 4) Access the primary unit, Tools->High Availability and click the HA Default button.

Step 5) Remove the secondary unit and all associated cabling

Appendix D - CLI Menu Overview

The EdgeXOS incorporates an SSH-based CLI menu (accessible via port 2022). This menu system provides the ability to conduct troubleshooting and modify existing configuration parameters.

```
19-Show Configuration File
20-Edit Configuration File
21-Reload Configuration File
```

Show Configuration File

This option will print to screen the existing configuration file:

```
Edge Configuration File

################################################################################
#
# Version XOS Version 3.4.3 Build 168
#
# Created on ... .... .. ..:..:.. ....., Serial Number
#
# Warning: Modifying and uploading this file will change the configuration.
#
################################################################################

# Registration - company, contact, email, phone, referece, wan1, wan2, wan3, wan4, wan5
#
# Example: REG,ABC,John Smith,jsmoth@abc.com,555-555-1212,1234,wan1,wan2,wan3,wan4,wan5


REG,[illegible]

# System Information - dns1_server, dns2_server, GMS_server, Overflow (1 = on, 0 = off)
#
# Example: SYSTEM,4.2.2.2,4.2.2.2,1544kbit,rac2.myxroads.com,1

SYSTEM,192.168.168.50,68.4.8.229,rac2.myxroads.com,
```

Edit Configuration File

This option provides the ability to add/delete or edit an existing configuration parameter.

To **add a parameter** simply enter to new rule and/or policy using the same syntax as provided within the shown configuration file.

Example: Firewall Rule

Adding a firewall rule would look like this:

FIREWALL,172.16.168.168,80,ANY,ANY,TCP,WAN1,DROP,wan_group

This would add a rule which dropped port 80 traffic coming in on WAN1 with a destination of 172.16.168.168.

The components of this line are detailed within the configuration file itself:

```
# Firewall - src addr, src port (or leave blank), dst addr, dst port (range [:] or leave blank), protocol, interface, action, rule group (no spaces)
```

To **edit a parameter** simply enter the line which would replace the existing parameter, make sure the parameter being changed is a standard parameter, i.e. pre-exists in the default configuration file.

Example: Interface parameters are default parameters

```
INT,lan,192.168.100.168,255.255.255.0,192.168.168.254,off,off,off,ACTIVE,,10000,,
INT,wan1,[illegible],255.255.248.0,[illegible],off,off,on,ACTIVE,100,10000kbit,10000kbitk,[illegible]
INT,wan2,,,,,255.255.255.0,,off,off,on,INACTIVE,100,10000kbit,10000kbitk,
```

You can modify these parameters simply by re-entering the line:

INT,wan1x.x.x.x,255.255.248.0,y.y.y.y,off,off,on,ACTIVE,100,10000kbit,10000kbitk,z.z.z.z

When the configuration file is reloaded these parameters will take effect over the previously entered parameters.

To **delete or remove a parameter** simply enter the line which you wish to remove and but add 'DEL-' to the beginning of the line. This will remove the parameter from the configuration upon the next reload.

Example: Traffic shaping policy

```
TSPOLICY,testing,test,,[illegible],dst
TSPOLICY,testing_reverse,test,,[illegible],src
```

DEL-TSPOLICY,testing,test,,xx.xx.xx.xx,,dst

NOTES: Currently some policies and rules can not be removed using the CLI menu system. These must be removed via the web interface. Additional capabilities are being added to this CLI so check back for future updates.

Full configuration changes can be made by downloading the configuration file, changing the text, and uploading the entire new configuration file. This can be done via the configuration file link on the home page.

Reload Configuration File

This option gives the end-user the ability to reload the configuration file once changes have been made. Reloading will immediately change the existing configuration file and it will automatically save the new configuration file.

WARNING: Reloading will also automatically update the running configuration in future releases, so be careful…

Appendix E - Glossary and Definitions

Term	Definition
BPR (Best Path Routing)	This is XRoads Networks next generation, patent pending method for network load balancing and optimizing application routing. More specifically, BPR allows customers to optimize critical routes between two or more offices with full path reporting which show the latency, packet loss, and calculated jitter between each location.
Vector Routing	This is the algorithm that is used to determine through which WAN connection network traffic is routed. This algorithm is affected by the utilization of each link, the previous DNS responses, WAN weighting (as determined by the administrator), specific application routing rules, and the current condition of each WAN connection.
ActiveDNS	This is the module responsible for editing and configuring the dynamic DNS system. All adjustments to the inbound (server) connections are handled via this module. This module is required for any inbound DNS based connectivity, redundancy and/or load balancing.
Traffic Shaping	A core feature of the EdgeXOS appliance, intelligent traffic shaping enables a network administrator to rate-limit traffic based on IP address, TCP/UDP port, network subnet, and URL. Bandwidth usage can be designated with a max and min bandwidth setting per policy. Additionally various priorities can be established to create very granular allocation of network bandwidth to specific applications.
Multi-WAN Aggregation & Network Load Balancing	The ability to balance network traffic over multiple connections. Balancing is session based, which means that each network session is balanced across the various active WAN connections. The balancing can be weighted and is adjusted based on utilization and critical path definitions. Example: When connecting to a web site, multiple sessions are opened

Term	Definition
	to download the text, and images of the site. Each session is balanced over the active WAN connections, thus decreasing the wait time for a site to be downloaded.
Multi-Level Outage Detection	This is the process in which we determine whether a WAN connection is up or down. Our patent pending method includes two phases, first we ping the gateway and the remote probe address (or the remote side of the WAN connection), then we further probe various core routers and core websites on the Internet to determine if an outage has occurred.
Inbound vs Outbound Load Balancing	Outbound load balancing is when LAN traffic is balanced across the various WAN connections. Inbound load balancing is when inbound server based connections are balanced via the ActiveDNS module. Each time an inbound request is made, the ActiveDNS module determines which WAN interface address to provide based on the current usage, and administrative preferences.
Site2Site Auto-Failover	There are many appliances on the market that provide secure virtual private networks (VPN) capabilities. A VPN is generally used to connect two or more locations via a secure tunnel so that the data passing between the two or more connections is highly secure. The problem with normal VPN appliances is that they are incapable of automatically failing over to a secondary VPN tunnel and WAN interface in the event that the primary VPN fails.
Virtual Technician	This trademarked feature provides the ability to actively and automatically troubleshoot a network failure. When a failure is detected by the WAN testing module, the Virtual Technician begins a series of tests in an attempt to determine the cause of the problem in order to assist with its resolution. Only XRoads Networks has this capability.
VirtualNAT	This is the XRoads Networks name for a Virtual Server (when a device proxies connections for another device). VirtualNAT is essentially a TCP proxy for LAN based servers and makes setting up inbound services a snap. The limitations of VirtualNAT are that all logging will appear to

Term	Definition
	come from the EdgeXOS appliance.
Vector Mapping	The process by which the EdgeXOS appliance ensures that inbound and outbound traffic flows are bonded to the correct WAN connection. If an inbound connection, destine for a server, does not go out the WAN interface which it came in on, the session could be dropped by either the ISP routers or firewall.
One-To-One vs. One-To-Many NAT	Network Address Translation (NAT) is designed to essentially translate an address on the WAN to an address on the LAN. For example NAT is commonly used to translate private space on the LAN to public space on the WAN. These two specific forms of NAT are designed to allow inbound connections, destine for a WAN address, to be forwarded to internal LAN addresses. One-To-One is designed translate all the ports of a WAN address to all of the ports of a LAN address, where One-To- Many only translates a single port on a WAN address to a single port on a LAN address.

Appendix F - How To Get Assistance

The easiest way to obtain assistance from XRoads Networks support department is to visit support HQ at www.myxroads.com

Via this website you can chat with support, open a ticket, review HowToGuides, and get answers to frequently asked questions.

International Support: Please contact your regional XRoads Networks distributor for additional information and assistance. Thank you.